

# Contents

## Skype for Business Server 2019

- What's new

- What's deprecated

- Microsoft telephony solutions

- Skype for Business downloads and updates

  - Client updates

  - Server updates

- Hybrid solutions for Teams and Skype for Business

- Plan

  - Topology Basics

    - Reference topologies

  - Requirements

    - System requirements

    - Load balancing requirements

    - Network requirements

      - IPv6

        - IP address types

      - DNS

        - Basics

        - Simple URLs

        - Advanced Edge Server DNS

      - Port and protocol requirements

  - Authentication and Authorization

    - Topologies supported

    - Server-to-server and partner applications

    - User and client authentication

  - Clients and devices

    - User experience

    - Desktop client feature comparison

- Mobile feature comparison
- Windows requirements
- Mac requirements
- Compatibility with Office
- Video resolutions
- Meetings clients
  - Skype Meetings App minimum network requirements
- VDI environments
- High availability and disaster recovery
  - High availability
  - Disaster recovery
  - User experience
  - Back End Server
  - File sharing
- Instant messaging and presence
- Video Interop Server
- Voice Solutions
  - Enterprise Voice
    - Components required for Enterprise Voice
      - Mediation Server
      - PSTN connectivity
      - Front End Server VoIP
    - PSTN connectivity
      - SIP trunking
      - Direct SIP
      - M:N trunk
      - Inter-trunk routing
      - Translation rules
      - Outbound voice routing
  - Enterprise Voice resiliency
  - Network settings for advanced features
  - Call admission control

- Example: Gathering requirements
- Components and topologies
- Emergency services
  - Define requirements
  - Multiple emergency numbers
- Media bypass
- Private telephone lines
- Location-Based Routing
  - LBR for Conferencing
- Call management features
  - Call Park
  - Group Call Pickup
  - Response Group
  - Announcement
- Shared Line Appearance
- Busy Options
- Call Via Work
- Remote call control
- Cloud Voicemail
  - Plan Cloud Voicemail
  - Configure Cloud Voicemail
- Cloud Auto Attendants
  - Plan Cloud auto attendants
  - Configure resource accounts
- Cloud Call Queues
  - Plan Cloud call queues
  - Configure resource accounts
- Plan to integrate Skype for Business and Exchange
- Unified Messaging
  - Deployment overview
- Unified contact store
- Plan for Skype for Business Server and Exchange Server migration

Exchange Unified Messaging Online migration support

Monitoring

Archiving

Conferencing

Hardware and software requirements

Conferencing topology

Dial-in conferencing

Large meetings

Edge Server deployments

System requirements

Edge environmental requirements

Advanced Edge Server DNS

Scenarios

Mobility

Security

Antivirus

Key security

Common threats

Security framework

Active Directory Domain Services

Role-based access control (RBAC)

Public Key Infrastructure for Skype

TLS and MTLS

Encryption

Management tools

Addressing threats

Capacity

User model

Estimating voice traffic

Mediation Server deployment guidelines

User models

Deploy

Install

- Install prerequisites
- Create a file share
- Install administrative tools
- Prepare Active Directory
- Create DNS records
- Create and publish new topology
- Install Skype for Business Server
- Verify the topology
- Deploy Call Via Work
- Deploy archiving
  - Add archiving databases
  - Configure archiving options
  - Configure archiving policies
  - Configure archiving disclaimers
  - Configure integration with Exchange storage
- Deploy monitoring
  - Associate a monitoring store
  - Install SQL Server Reporting Services
  - Install Monitoring Reports
  - Monitoring Reports with a mirror database
  - Call detail recording and QoE
  - Purgecall detail recording and QoE
- Deploy Video Interop Server
  - Create a VIS pool
  - Deploy the VIS server role
  - Configure the VIS
  - Configure CUCM for Interoperation
  - Configure a VTC for Interoperation
- Deploy Enterprise Voice
  - Enterprise Voice security
  - Deploy a Mediation Server
  - Define a gateway

Define additional trunks

Install Mediation Server

Configure trunks

- Configure trunk (with media bypass)

- Configure trunk (without media bypass)

- Trunk configuration settings

- Delete trunk configuration

- Modify SIP trunk configuration

- Test SIP trunk configuration

- View SIP info

Caller ID presentation rules

Called ID presentation rules

Normalization rules

Dial plans

Voice and PSTN

- Voice policy and PSTN usage records

- Configure voice mail escape

- View PSTN usage records

- Create or modify a voice route

- Voice route configuration import/export

- Voice route config changes

Enable users for Enterprise Voice

Deploy advanced Enterprise Voice features

- Deploy network

- Deploy call admission control

  - Create bandwidth policy profiles

  - Create network region links

  - Create network interregional routes

  - Create network intersite policies

  - Enable call admission control

  - Final checklist

- Deploy emergency services

- Configure an E9-1-1 voice route
- Create location policies
- Add a location policy to a network site
- Configure the location database
- Configure an SNMP application
- Secondary Location Information service
- Configure multiple emergency numbers

#### Deploy media bypass

- Bypass the Mediation Server
- Use site and region information

#### Deploy call management features

##### Deployment process for Call Park

- Create or modify a Call Park orbit range
- Configure Call Park settings
- Customize Call Park music on hold
- Enable Call Park for users
- Verify normalization rules for Call Park
- (Optional) Verify Call Park deployment

##### Deployment process for Group Call Pickup

- Deploy the SEFAUtil tool
- Create or modify a Group Call Pickup number range
- Enable Group Call Pickup for users and assign a group number

##### Deployment process for Response Group

- Create or modify an agent group
- Create or modify a queue
- (Optional) Define Response Group business hours
- (Optional) Define Response Group holiday sets
- Designing and creating response group workflows
- Managing application-level Response Group settings
- (Optional) Verify Response Group deployment

##### Deployment process for the Announcement application

- Create an announcement

- Create or modify an unassigned number range
- (Optional) Verify Announcement deployment
- Deploy Shared Line Appearance
- Install and configure Busy Options
- Integrate with Exchange Server
  - Configure partner applications
  - Use Exchange archiving
  - SharePoint to search for archived data
  - High-resolution photos
  - Use the unified contact store
  - Exchange Unified Messaging for voice mail
  - Outlook Web App
  - OAuth with Online and On Premises
  - Deploy unified contact store
- Deploy Skype Connectivity
- Deploy conferencing
  - Office Web App Server
  - Dial-in conferencing
  - Room System v1 Administrative Web Portal
- Deploy Edge Server
  - Create your Edge topology
  - Deploy Edge Servers
  - Validate Edge deployment
- Deploy and configure Mobility
- Deploy clients
  - Customize Windows client installation
    - Use the Office Customization Tool (OCT)
    - Use Config.xml to perform installation tasks
    - Use Setup command-line options
    - Configure client bootstrapping policies
- iOS
  - Configure Smart contacts list



Deploy Web downloadable clients

Customize the Mac client experience

Configure Skype Meeting Broadcast

IM and presence

Enable or Disable Offline IM

Deploy high availability and disaster recovery

AlwaysOn Availability Group

Front End pools for disaster recovery

Migrate

Before you begin the migration

Migration process

Migration phases

Phase 1: Plan your migration

User migration

Migrating Archiving and Monitoring servers

Administering servers after migration

Migrating multiple sites and pools

Migrating XMPP federation

Phase 2: Prepare for migration

Apply updates to legacy installation

Configure DNS records for pilot pool deployment

Back up systems and data

Configure clients for migration

Verify legacy environment you are migrating from

Phase 3: Deploy pilot pool

Prepare Active Directory for pilot pool

Download topology from existing deployment

Deploy pilot pool

Verify pilot pool coexistence with legacy pool

Connect pilot pool to legacy Edge Servers

Configure XMPP gateway access policies and certificates

Phase 4: Move test users to pilot pool

- View current users in legacy pool
- Verify user replication has completed
- Move a single user to pilot pool
- Move multiple users to pilot pool

#### Phase 5: Add Edge Server to pilot pool

- Deploy pilot Edge Server
- Verify configuration settings

#### Phase 6: Move from pilot deployment into production

- Configure federation routes and media traffic
- Verify federation and remote access for external users
- Change simple URLs after migration
- Move remaining users

#### Phase 7: Complete post-migration tasks

- Migrate existing meetings and meeting content
- Migrate dial-in access numbers
- Migrate Call Park application settings
- Migrate response groups
- Migrate Address Book
- Configure the meeting join page
- Remove legacy Archiving and Monitoring servers
- Configure trusted application servers
- Deploy Skype for Business clients
- Connect a Survivable Branch Appliance
- Configure SCOM monitoring
- Migrate Common Area Phones
- Migrate analog devices

#### Phase 8: Decommission legacy pools

- Update DNS SRV records
- Move the legacy Central Management Server
- Move Conference Directories
- Remove the Archiving server association
- Remove the Monitoring server association

Remove the Front End Server

- Reset call admission control

- Prevent sessions for services

- Stop legacy services

- Remove a Front End Server from a pool

- Remove Front End pool or Standard Edition server

Remove SQL Server instances and databases on the Back End Server

- Remove the SQL Server database for a Front End pool

- Remove the SQL Server database for a Monitoring server

- Remove the SQL Server database for an Archiving server

Manage

Topology

- Manage Front End Servers

- Patch or update a Back End or Standard Edition server

- Manage databases

- Move File Store Data

- Disable TLS 1.0/1.1

Health and monitoring

- Access monitoring data

- Call detail recording (CDR)

  - View configuration information

  - Enable CDR

  - Specify retention of data

  - Create or modify a collection of CDR configuration settings

  - Delete an existing collection of CDR configuration settings

Quality of Experience

- Create QoE configuration settings

- Enable QoE

- Modify QoE settings

- Delete QoE configuration settings

Monitor mobility performance

- Server memory capacity limits

Service and UCWA usage

Configure Service

Performance counters

UCWA events

Monitoring Reports

Monitoring Dashboard

System usage reports

User Registration Report

Peer-to-Peer Activity Summary Report

Conference Summary Report

PSTN Conference Summary Report

Response Group Usage Report

IP Phone Inventory Report

Call Admission Control Report

Call Diagnostic Reports (per user)

Call Diagnostic Reports

Summary Report

Peer-to-Peer Activity Diagnostic Report

Conference Diagnostic Report

Top Failures Report

Failure Distribution Report

Failure List Report

Diagnostic Report

Media Quality Diagnostic Reports

Summary

Comparison

Server Performance

Location Report

Device Report

Call List Report

Call Detail Report

Server Media Quality Trend Report

Media Quality Metrics Distribution Report

Location Trend Report

Rate my Call

Call Data Connector

Plan Call Data Connector

Configure Call Data Connector

Archiving

Options

Create a configuration

Delete a configuration

Enable or disable archiving

Configure options to handle failures

Purging of archived data

Policies

Create a new policy

Change an existing policy

Apply a policy to users

Delete an existing policy

Change Archiving database options

Export archived data

Conferencing

Conferencing policies

View

Create policies

Modify policies

Assign policies

Delete policies

Meeting configuration settings

View settings

Create settings

Modify settings

Delete settings

## Conferencing server configuration settings

### Dial-in conferencing

- Enable or disable

- Access numbers

- PIN policies

- Join and leave announcements

- Key mapping for DTMF commands

- PIN-less meeting join

- Directories

- Welcome emails

- Tests

### Meeting join page

## Management Shell

### Authentication

- Use ADAL

- Stage AV and OAuth certificates

- Assign a server-to-server certificate

- Configure server-to-server authentication for hybrid

- Configure an on-premises partner app

- Registrar configuration settings

- Web Service configuration settings

### PIN settings

- View PIN policy information

- Create a new PIN policy

- Modify an existing PIN policy

- Delete a PIN policy

- Assign a per-user PIN policy

- Set a user's dial-in conferencing PIN

- View user PIN information

- Lock or unlock a user PIN

### Two-factor authentication

- Configure two-factor authentication

Use two-factor authentication

Video based Screen Sharing for Skype for Business Server

User accounts

    Customize properties

Manage services

Back-up RGS Data

Using SEFAUtil

Management Tools

Call Quality Dashboard for Skype for Business Server

    Plan for Call Quality Dashboard

    Deploy Call Quality Dashboard

    Use Call Quality Dashboard

Statistics Manager for Skype for Business Server

    Plan for Statistics Manager for Skype for Business Server

    Deploy Statistics Manager for Skype for Business Server

    Upgrade Statistics Manager for Skype for Business Server

    Troubleshoot Statistics Manager for Skype for Business Server

Manage Skype for Business Server using SCOM Management pack

    Configure the Primary Management Server

    Configure computers to be monitored

    Watcher nodes

        Test users and settings

Skype for Business Server Capacity Planning Calculator

[Plan](#)

[Hybrid solutions](#)

[Deploy](#)

[Upgrade](#)

[Manage](#)

[Download now!](#)

#### Featured articles

<b>Before you start</b> <a href="#">System requirements</a> <a href="#">Network requirements</a>	<b>Install</b> <a href="#">Install Skype for Business Server</a> <a href="#">Migrate to Skype for Business 2019</a>	<b>Enterprise Voice</b> <a href="#">Plan</a> <a href="#">Deploy</a>
<b>New features</b> <a href="#">What's new</a>	<b>Hybrid solutions</b> <a href="#">Plan hybrid connectivity</a>	<b>Prior releases</b> <a href="#">Skype for Business Server 2015 documentation</a> <a href="#">Lync Server 2013 documentation</a>



# What's in Skype for Business Server 2019

5/20/2019 • 2 minutes to read

**Summary:** Read this topic to learn about new features in Skype for Business Server 2019.

New features in Skype for Business Server 2019 include the following:

- Cloud Voicemail
- Call Data Connector
- Side-by-side migration

## Unified messaging services: Cloud Voicemail

Exchange UM remains available in Skype for Business Server 2019 when you integrate Skype for Business 2019 with Exchange 2013 or Exchange 2016. Due to changes in support in Exchange 2019, Exchange UM integration is being de-emphasized in favor of Cloud Voicemail and Cloud Auto Attendant features.

Cloud Voicemail enables all your Skype for Business 2019 users—whether they are homed on premises or online—to have access to the same voicemail service in the Microsoft Cloud. Cloud Voicemail provides the following benefits for both your on-premises and online users:

- Access to voicemail in their Exchange mailbox by using the Skype for Business Online, Teams, or Outlook clients
- Ability to use the web-based portal to manage their voicemail options

See [Plan Cloud Voicemail service](#) and [Plan for Skype for Business Server and Exchange Server migration](#) for more information.

## Call monitoring: Call Data Connector

Call Data Connector greatly simplifies call monitoring in a hybrid environment because you no longer need to use different sets of on-premises and online tools to monitor all of your users call quality. Whether your users are homed on premises or online, you can choose to view call quality for your entire organization online.

With Call Data Connector, you can perform the following tasks by using a single toolset:

- Monitor your user experience across Microsoft Teams, Skype for Business Online, and Skype for Business Server.
- View and troubleshoot problems across your network
- Assign helpdesk and administrator roles for Call Analytics, so that you can empower helpdesk workers to view and troubleshoot their areas of responsibility.

See [Plan Call Data Connector](#) for more information.

### See also

[What's deprecated from Skype for Business Server 2019](#)

# What's deprecated from Skype for Business Server 2019

7/1/2019 • 2 minutes to read

Learn about the features and functionality that are deprecated in Skype for Business Server 2019. For information about new features in Skype for Business Server 2019, see [What's in Skype for Business Server 2019](#).

Some de-emphasized features are included in Skype for Business Server 2019 for compatibility with previous product versions.

## Features deprecated in Skype for Business Server 2019

The following features and functionality have been deprecated in Skype for Business Server 2019.

### **XMPP Gateways for Skype for Business Server**

Skype for Business Server 2015 and its predecessors allowed you to configure an Extensible Messaging and Presence Protocol (XMPP) proxy on the Edge Server and an XMPP Gateway on the Front End Server or Front End pool. This functionality is no longer available in Skype for Business Server 2019.

### **Persistent Chat for Skype for Business Server**

Persistent Chat Server is an optional role that lets multiple users in your organization participate in chat room conversations that persist over time. Persistent chat can't be deployed with Skype for Business Server 2019. This server role is removed from Topology Builder, as well as from the code.

The same functionality is available in Teams. For more information, see [Getting started with your Microsoft Teams upgrade](#).

### **SQL Mirroring for Skype for Business Server**

SQL Mirroring can't be deployed with Skype for Business Server 2019. Other options for providing High Availability and Disaster Recovery are still supported and you should choose from among them. See [Plan for high availability and disaster recovery in Skype for Business Server](#) to review the options.

### **In-place upgrades**

In-place upgrades were available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. Side by side upgrade and coexistence is supported, see [Migration to Skype for Business Server 2019](#) for more information.

### **Mobility Service (Mcx)**

Mobility Service support used by legacy mobile clients is no longer available in Skype for Business Server 2019. This was previously announced in Skype for Business Server 2015.

All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using Mcx will need to upgrade to a current client.

For more details, see [Plan for Mobility for Skype for Business Server](#) and [Mobile client feature comparison for Skype for Business](#).

## Tools

The following tools will not be available for use at the initial release of Skype for Business Server 2019:

- Skype for Business Server Capacity Planning Calculator
- Skype for Business Server Debugging Tools
- Skype for Business Server Resource Kit Tools (some tools will be removed)
  - Call Parkometer
  - Lookup user console
  - Unassigned number Announcement Migration

The following tools are not supported with Skype for Business Server 2019:

- Call Quality Methodology (but not Call Quality Dashboard)
- Microsoft Call Quality Methodology Scorecard, v1.5
- Skype for Business Server 2015 Planning Tool
- Skype for Business Server 2015 Stress and Performance Tool

**See also**

[What's new in Skype for Business Server 2019](#)

[Migrating XMPP federation](#)

# Microsoft telephony solutions

5/20/2019 • 8 minutes to read

Microsoft supports several options as you begin your journey to Teams in the Microsoft cloud. This article helps you decide which Microsoft telephony solution (Phone System in the cloud or Enterprise Voice on-premises) is right for users in your organization, and how your organization can connect to the Public Switched Telephone Network (PSTN).

You should use this article along with the associated technical diagram, which provides a visual aid for making the right decision for your organization:

- [Microsoft telephony solutions - PDF](#)
- [Microsoft telephony solutions - Visio](#)

## Private Branch Exchange (PBX) options

### Phone System (Office 365)

Phone System is Microsoft's technology for enabling call control and Private Branch Exchange (PBX) capabilities in the Office 365 cloud with Microsoft Teams and/or Skype for Business Online.

Phone System works with Teams or Skype for Business Online clients and certified devices. Phone System allows you to replace your existing PBX system with a set of features directly delivered from Office 365 and tightly integrated into the company's cloud productivity experience. To connect Phone System to the Public Switched Telephone Network (PSTN), you can choose Microsoft's Calling Plan or your own telephony carrier.

For more information, see [What is Phone System in Office 365](#).

### Enterprise Voice (Skype for Business Server)

Enterprise Voice is Microsoft's technology for enabling call control and Private Branch Exchange (PBX) capabilities in the on-premises Skype for Business Server. This option can only be connected to the Public Switched Telephone Network by using your own telephony carrier.

For more information, see [Plan for Enterprise Voice in Skype for Business Server](#).

## Connection to the Public Switched Telephone Network (PSTN) options

You can choose to connect to the Public Switched Telephone Network (PSTN) by:

- Using Microsoft Calling Plan in Office 365
- Connecting your own telephony carrier

### Calling Plan (Office 365)

This option connects Microsoft's Office 365 Phone System to the Public Switched Telephone Network (PSTN) to enable calls to landlines and mobile phones around the world. With Calling Plan, Microsoft is your PSTN carrier.

For more information, see [Calling Plans for Office 365](#).

### Connect your own telephony carrier (Office 365 and Skype for Business on-premises)

This option connects either Phone System in Office 365 or Enterprise Voice system in Skype for Business on-premises to your telephony network. This option requires a supported Session Border Controller (SBC). In some cases, this option might require additional Microsoft software deployed on-premises.

# Which solution is right for your organization?

You can choose an all-in-the-cloud solution, a connect-your-own-carrier solution, or a mix between all-in-the-cloud and third-party carriers:

- Phone System with Calling Plan (all in the cloud)
- Phone System with own carrier via Direct Routing
- Phone System with own carrier via Skype for Business Server OR Cloud Connector Edition
- Enterprise Voice in Skype for Business Server with own carrier

The solution you choose depends on your current and future needs, such as:

- Whether you want—or are required—to retain functionality provided by your on-premises deployment.
- Which client you want to deploy for your users.
- What your plan is for moving people to the cloud.
- Whether you need to interoperate with 3rd party PBXs and other telephony equipment.

Consider the following questions to determine the best solution for your organization:

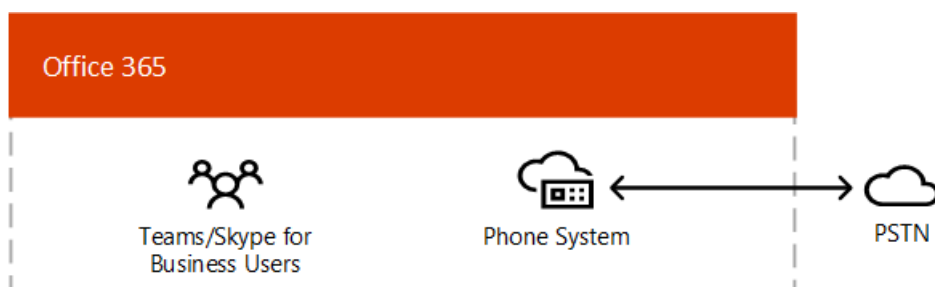
- Do you have an existing Skype for Business Server deployment?
- Are your users homed in Skype for Business on premises, in the cloud on Skype for Business Online, or both?
- Do you want to move on-premises users to the cloud?
- Is Microsoft's PSTN Calling Plan available in your region?
- Do you want or need to keep your current telephony carrier? For example, do you need to keep your current carrier because of an existing contract?
- Do you have an existing on-premises legacy PBX that you want or need to keep?
- Does your current legacy PBX offer unique features that are critical to your business?
- Do any or all of your users require features not currently offered in Phone System?

Note the following:

- All four options can co-exist with each other in case you need to design a solution for complex environment or managing multi-step migration.
- Phone System with own carrier via Skype for Business Server OR Cloud Connector Edition can only be deployed with either Skype for Business Server OR Cloud Connector. Co-existence of Skype for Business Server and Cloud Connector is not supported in a single company.

## Phone System with Calling Plan

Phone System with Calling Plan is an all-in-the-cloud option for Teams or Skype for Business Online users as shown in the following diagram:



- Microsoft Phone System with added Domestic or International Calling Plans that enables calling to phones around the world (depending on the level of service being licensed).
- Because PSTN Calling Plan operates out of Office 365, this option does not require deployment or maintenance

of any on-premises deployment.

- Customers can connect a supported SBC via Direct Routing for interoperability with 3rd party PBX, analog devices, and other 3rd party telephony equipment supported by the SBC.

INFRASTRUCTURE REQUIREMENTS	REQUIRED?
Requires uninterrupted connection to Office 365	Yes
Available worldwide*	No
Requires deploying and maintaining a supported Session Border Controller (SBC)	No
Requires contract with third-party carrier	No
Requires deploying and maintaining Skype for Business Server or Cloud Connector Edition	No

\* For more information about the countries where Calling Plan is available, see [Country and region availability for Audio Conferencing and Calling Plans](#).

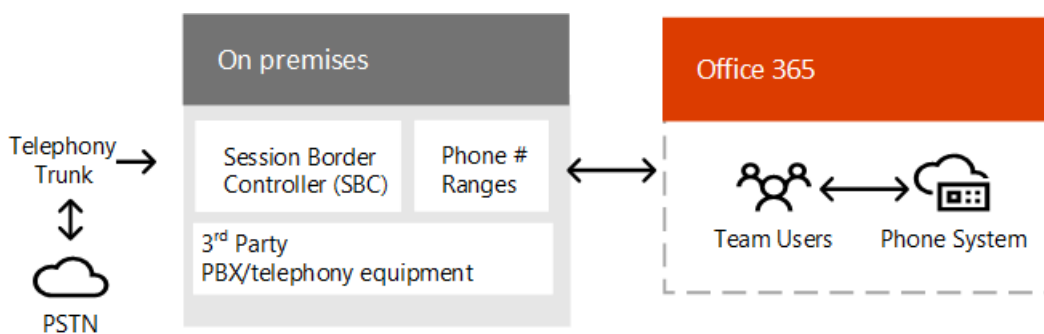
If you answer yes to the following questions, then this is the right solution for you:

- Calling Plan is available in your region.
- You do not need to retain your current PSTN carrier.
- You want to use Microsoft-managed access to the Public Switched Telephone Network( PSTN).
- You do not want to manage Session Border Controllers on your own.
- Teams and/or Skype for Business Online has all the features that your organization requires.

For more information, see [What is Phone System in Office 365](#) and [Calling Plans for Office 365](#).

## Phone System with own carrier via Direct Routing

This option provides Microsoft Phone System in the cloud with virtually any telephony carrier for Teams users.



- Connect your own supported SBC to Microsoft Phone System directly without need of additional on-premises software.
- Use virtually any telephony carrier with Microsoft Phone System.
- Can be configured and managed by customers or by your carrier or partner (ask if your carrier or partner provides this option).
- Configure interoperability between your telephony equipment—such as a third-party PBX and analog devices—and Microsoft Phone System.

INFRASTRUCTURE REQUIREMENTS	REQUIRED?
Requires uninterrupted connection to Office 365	Yes
Available worldwide	Yes
Requires deploying and maintaining a supported Session Border Controller (SBC)	Yes
Requires contract with third-party carrier*	Yes
Requires deploying and maintaining Skype for Business Server or Cloud Connector Edition	No

\* Unless deployed as an option to provide connection to 3rd party PBX, analog devices, or other telephony equipment for users who are on Phone System with Calling Plans.

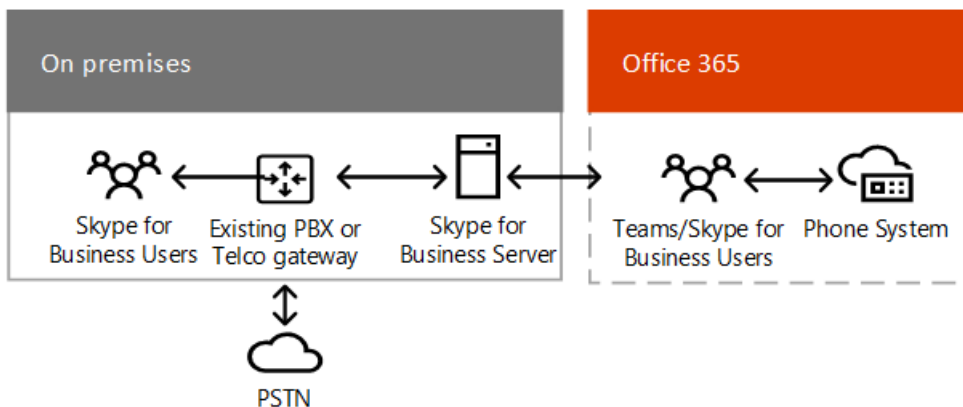
If you answer yes to the following questions, then this is the right solution for you:

- You want to use Teams with Phone System.
- You need to retain your current PSTN carrier.
- You want to mix routing, some calls are going via Calling Plans, some via your carrier
- You need to interoperate with 3rd party PBXs and/or equipment such as overhead pagers, analog devices
- Teams has all the features that your organization requires.

For more information, see [What is Phone System in Office 365](#) and [Plan Direct Routing](#).

## Phone System with own carrier via Skype for Business Server OR Cloud Connector Edition

This option provides Microsoft Phone System in the cloud with connectivity to an on-premises telephony network for Skype for Business Online users.



- Connect your own supported SBC to Microsoft Phone System via Skype for Business Server or Skype for Business Cloud Connector Edition deployed on-premises.
- Use virtually any telephony carrier with Microsoft Phone System.
- If you already have Skype for Business Server on-premises you can leverage it; if you do not, you can deploy a lighter version – Cloud Connector Edition.

INFRASTRUCTURE REQUIREMENTS	REQUIRED?
Requires uninterrupted connection to Office 365	Yes
Available worldwide	Yes
Requires deploying and maintaining a supported Session Border Controller (SBC)	Yes
Requires contract with third-party carrier	Yes
Requires deploying and maintaining Skype for Business Server or Cloud Connector Edition	Yes

If you answer yes to the following questions, then this is the right solution for you:

- You want to use Skype for Business Online for your users.
- PSTN Calling Plan is not available in your region.
- You need to retain your current PSTN carrier.

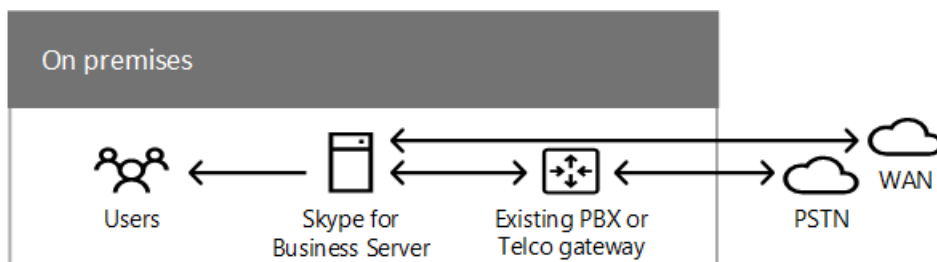
For more information, see [What is Phone System in Office 365](#), [Skype for Business Server 2019](#), and [Plan for Skype for Business Cloud Connector Edition](#).

Recommendation: When business conditions change--for example, you no longer need to retain your PSTN carrier--consider moving to Microsoft Teams using options 1 or 2 to:

- Minimize maintenance costs
- Have access to the latest features released by Microsoft

## Enterprise Voice in Skype for Business Server with own carrier

This option provides Enterprise Voice on-premises with connectivity to an on-premises telephony network for Skype for Business on-premises users.



- Connect your own supported SBC to Enterprise Voice System in Skype for Business on-premises Server.
- Use if you need local survivability.
- Use virtually any telephony carrier with Microsoft Phone System.
- Most complex option to deploy and maintain.

INFRASTRUCTURE REQUIREMENTS	REQUIRED?
Requires uninterrupted connection to Office 365	No
Available worldwide	Yes



INFRASTRUCTURE REQUIREMENTS	REQUIRED?
Requires deploying and maintaining a supported Session Border Controller (SBC)	Yes
Requires contract with third-party carrier	Yes
Requires deploying and maintaining Skype for Business Server	Yes

For more information, see [Plan for Enterprise Voice in Skype for Business Server](#).

Recommendation: When business conditions change--for example, you no longer need to retain your PSTN carrier--consider moving to Microsoft Teams using options 1 or 2 to:

- Minimize maintenance costs
- Have access to the latest features released by Microsoft

# Skype for Business downloads and updates

11/19/2019 • 2 minutes to read

The *Skype for Business downloads and updates* web page that was once on Technet has been retired. The content was reorganized into client and server pages. Follow these links to the content you need:

- [Updates for Skype for Business clients](#) which contains the sections:
  - [Skype for Business 2016 client updates](#)
  - [Skype for Business 2015 client updates](#)
  - [Skype for Business on Mac client updates](#)
  - [Lync 2013 client updates](#)
    - [Lync Phone Edition updates](#)
    - [Lync Phone Edition clients on Download Center](#)
    - [Lync Basic 2013 Trial Software](#)
  - [Lync for Mac 2011 client updates](#)
  - [Lync 2010 client updates](#)
    - [Lync 2010 Attendant updates](#)
    - [Lync 2010 Attendee updates](#)
- [Skype for Business Server updates](#) which contains the sections:
  - [Skype for Business Server 2019 update history](#)
  - [Skype for Business Server 2015 update history](#)
  - [Lync Server 2013 update history](#)
    - [Lync Server 2013 Dev tools](#)
    - [Pre-configured VHDs](#)
    - [Lync 2013 Tools](#)
    - [Lync 2013 downloadable documentation](#)
  - [Lync Server 2010 update history](#)
    - [Group Chat 2010 updates](#)
    - [Lync 2010 Dev Tools](#)
    - [Lync 2010 Tools](#)
    - [Lync 2010 downloadable documentation](#)
    - [Resource kit \(technical reference\)](#)
    - [Group Chat](#)
    - [Trial Software](#)
  - [Additional information](#)
  - [Related topics](#)

# Latest updates for versions of Skype for Business that use Windows Installer (MSI)

12/16/2019 • 13 minutes to read

Use the links on this page to get more information about and download the most recent updates for the perpetual versions of Skype for Business 2016, Skype for Business 2015, and Lync 2013 clients.

## NOTE

- The information in this article only applies to perpetual versions of Skype for Business that use the Windows Installer (MSI) installation technology. For example, if you installed a volume licensed version of Skype for Business, such as Skype for Business included with Office Professional Plus 2016.
- The information in this article doesn't apply to Office 365 versions of Skype for Business, such as Skype for Business included with Office 365 ProPlus.
- For the latest mobile client updates, go to the app store for your mobile client (iTunes, Google Play, or Microsoft Store) to view details and install updates.
- To find out what version of Skype for Business you're using, see [What version of Skype for Business do I have?](#)
- For more information about installing Office updates, see [Install Office updates](#).

Skype for Business compatibility with Office 365 and your on-premises environment depends on the system requirements for your deployment:

- Office 365 works with any version of Skype for Business that is in mainstream support, which includes the latest version of Skype for Business 2016. For previous versions of Skype for Business, only those that have extended support may continue to work with Office 365, although with reduced functionality. For more information, see [Microsoft Lifecycle Policy](#).
- For Skype for Business Server on-premises deployments, follow the system requirements for your version of Skype for Business:
  - [Requirements for your Skype for Business environment](#)
  - [Lync Server 2013 system requirements](#)

## Skype for Business 2016 client updates

- [Latest Updates for Skype for Business 2016](#)

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Skype for Business 2016	<a href="#">KB 4484102</a>	October 2019
Update for Skype for Business 2016	<a href="#">KB 4475577</a>	September 2019
Update for Skype for Business 2016	<a href="#">KB 4475548</a>	August 2019
Update for Skype for Business 2016	<a href="#">KB 4475545</a>	July 2019
Update for Skype for Business 2016	<a href="#">KB 4464576</a>	June 2019

<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Update for Skype for Business 2016	<a href="#">KB 4464532</a>	May 2019
Update for Skype for Business 2016	<a href="#">KB 4462234</a>	April 2019
Update for Skype for Business 2016	<a href="#">KB 4462190</a>	March 2019
Update for Skype for Business 2016	<a href="#">KB 4462114</a>	February 2019
Update for Skype for Business 2016	<a href="#">KB 4461586</a>	January 2019
Update for Skype for Business 2016	<a href="#">KB 4461545</a>	December 2018
Security update for Skype for Business 2016	<a href="#">KB 4461473</a>	November 2018
Update for Skype for Business 2016	<a href="#">KB 4092445</a>	October 2018
Update for Skype for Business 2016	<a href="#">KB 4032255</a>	August 2018
Security update for Skype for Business 2016	<a href="#">KB 4022221</a>	July 2018
Update for Skype for Business 2016	<a href="#">KB 4022155</a>	June 2018
Update for Skype for Business 2016	<a href="#">KB 4018367</a>	May 2018
Update for Skype for Business 2016	<a href="#">KB 4018323</a>	April 2018
Update for Skype for Business 2016	<a href="#">KB 4011725</a>	March 2018
Update for Skype for Business 2016	<a href="#">KB 4011662</a>	February 2018
Update for Skype for Business 2016	<a href="#">KB 4011623</a>	January 2018
Update for Skype for Business 2016	<a href="#">KB 4011563</a>	December 2017
Update for Skype for Business 2016	<a href="#">KB 4011238</a>	November 2017
Security update for Skype for Business 2016	<a href="#">KB 4011159</a>	October 2017
Security update for Skype for Business 2016	<a href="#">KB 4011040</a>	September 2017
Update for Skype for Business 2016	<a href="#">KB 3213548</a>	July 2017
Security update for Skype for Business 2016	<a href="#">KB 3203382</a>	June 2017
Security update for Skype for Business 2016	<a href="#">KB 3191858</a>	May 2017

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Skype for Business 2016	<a href="#">KB 3178717</a>	April 2017
Security update for Skype for Business 2016	<a href="#">KB 3178656</a>	March 2017
Update for Skype for Business 2016	<a href="#">KB 3141501</a>	February 2017
Update for Skype for Business 2016	<a href="#">KB 3128049</a>	January 2017
Update for Skype for Business 2016	<a href="#">KB 3127980</a>	December 2016
Update for Skype for Business 2016	<a href="#">KB 3127939</a>	November 2016
Security update for Skype for Business 2016	<a href="#">KB 3118327</a>	October 2016
Update for Skype for Business 2016	<a href="#">KB 3118288</a>	September 2016
Security update for Skype for Business 2016	<a href="#">KB 3115408</a>	August 2016
Update for Skype for Business 2016	<a href="#">KB 3115268</a>	July 2016
Update for Skype for Business 2016	<a href="#">KB 3115087</a>	June 2016
Security update for Skype for Business 2016	<a href="#">KB 3114960</a>	April 2016
Update for Skype for Business 2016	<a href="#">KB 3114846</a>	March 2016
Update for Skype for Business 2016	<a href="#">KB 3114696</a>	February 2016
Update for Skype for Business 2016	<a href="#">KB 3114516</a>	January 2016
Security update for Skype for Business 2016	<a href="#">KB 3114372</a>	December 2015
Security update for Skype for Business 2016	<a href="#">KB 3085634</a>	November 2015
Security update for Skype for Business 2016	<a href="#">KB 2910994</a>	September 2015

## Skype for Business 2015 client updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4475519</a>	July 2019

<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4464593</a>	June 2019
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4464547</a>	May 2019
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4462207</a>	April 2019
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4461557</a>	January 2019
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4461487</a>	November 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4461446</a>	October 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4092457</a>	September 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4032250</a>	August 2018
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4022225</a>	July 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4022170</a>	June 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4018377</a>	May 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4018334</a>	April 2018]
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4018290</a>	March 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011678</a>	February 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011638</a>	January 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011284</a>	December 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011255</a>	November 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011179</a>	October 2017

<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011107</a>	September 2017
Lynchelploc Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3213568</a>	September 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011046</a>	August 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3213574</a>	July 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191939</a>	June 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191937</a>	June 2017
Lynchelploc update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191873</a>	May 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191876</a>	May 2017
Lynchelploc update for Skype for Business 2015/Lync 2013	<a href="#">KB 3172492</a>	April 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3178731</a>	April 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3172539</a>	March 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3161988</a>	February 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3141468</a>	January 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3127976</a>	December 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3127934</a>	November 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3118348</a>	October 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3118281</a>	September 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3115431</a>	August 2016

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3115261</a>	July 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3115033</a>	June 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114944</a>	April 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114831</a>	March 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114732</a>	February 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114502</a>	January 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114351</a>	December 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3039776</a>	December 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3101496</a>	November 2015
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3085581</a>	October 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3085500</a>	September 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3055014</a>	August 2015
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3054791</a>	June 2015

### Skype for Business on Mac client updates

[Current release notes for Skype for Business on Mac](#)

### Lync 2013 client updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4462207</a>	April 2019
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4461557</a>	January 2019



<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4461487</a>	November 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4461446</a>	October 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4092457</a>	September 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4032250</a>	August 2018
Security update for Skype for Business/Lync 2013	<a href="#">KB 4022225</a>	July 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4022170</a>	June 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4018377</a>	May 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4018334</a>	April 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4018290</a>	March 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011678</a>	February 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011638</a>	January 2018
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011284</a>	December 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011255</a>	November 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011179</a>	October 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011107</a>	September 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3213568</a>	September 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 4011046</a>	August 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3213574</a>	July 2017

<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191939</a>	June 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191937</a>	June 2017
Lynchelploc update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191873</a>	May 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3191876</a>	May 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3172492</a>	April 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3178731</a>	April 2017
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3172539</a>	March 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3161988</a>	February 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3141468</a>	January 2017
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3127976</a>	December 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3127934</a>	November 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3118348</a>	October 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3118281</a>	September 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3115431</a>	August 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3115261</a>	July 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3115033</a>	June 2016
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114944</a>	April 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114831</a>	March 2016

<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114732</a>	February 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114502</a>	January 2016
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3039776</a>	December 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3114351</a>	December 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3101496</a>	November 2015
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3085581</a>	October 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3085500</a>	September 2015
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 3054791</a>	June 2015
Security update for Skype for Business 2015/Lync 2013	<a href="#">KB 3039779</a>	May 2015
Update for Skype for Business 2015/Lync 2013	<a href="#">KB 2889923</a> <a href="#">KB 2889853</a>	April 2015
Update for Lync 2013	<a href="#">KB 2956174</a>	March 2015
Update for Lync 2013	<a href="#">KB 2920744</a>	February 2015
Update for Lync 2013	<a href="#">KB 2899507</a>	November 2014
Update for Lync 2013	<a href="#">KB 2889929</a>	October 2014
Update for Lync 2013	<a href="#">KB 2889860</a>	September 2014
Update for Lync 2013	<a href="#">KB 2881083</a>	August 2014
Update for Lync 2013	<a href="#">KB 2881070</a>	August 2014
Security Update for Lync 2013	<a href="#">KB 2881013</a>	June 2014
Update for Lync 2013	<a href="#">KB 2850074</a>	June 2014
Update for Lync 2013	<a href="#">KB 2880980</a>	May 2014
Update for Lync 2013	<a href="#">KB 2880474</a>	April 2014

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Lync 2013	<a href="#">KB 2863908</a>	March 2014
Security Update for Lync 2013	<a href="#">KB 2850057</a>	September 2013
Update for Lync 2013	<a href="#">KB 2817630</a>	December 2013
Update for Lync 2013	<a href="#">KB 2817465</a>	July 2013
Update for Lync 2013	<a href="#">KB 2768004</a>	May 2013
Update for Lync 2013	<a href="#">KB 2760556</a>	March 2013
Update for Lync 2013	<a href="#">KB 2812461</a>	February 2013

### Lync Phone Edition updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Cumulative update for Lync Phone Edition for Aastra 6721ip and Aastra 6725ip telephone	<a href="#">KB 4019527</a>	April 2017
Cumulative update for Microsoft Lync Phone Edition for HP 4110 and HP 4120 telephones	<a href="#">KB 4019528</a>	April 2017
Cumulative update for Microsoft Lync Phone Edition for Polycom CX500, Polycom CX600, and Polycom CX3000 telephones	<a href="#">KB 4019529</a>	April 2017
Cumulative Update for Lync Phone Edition for Aastra 6721ip and Aastra 6725ip telephones	<a href="#">KB 3050585</a>	May 2015
Cumulative update for Lync Phone Edition for HP 4110 and HP 4120 telephones	<a href="#">KB 3050587</a>	May 2015
Cumulative update for Lync Phone Edition for Polycom CX500, Polycom CX600, and Polycom CX3000	<a href="#">KB 3050588</a>	May 2015
Cumulative update for Lync Phone Edition for Polycom CX700 and LG-Nortel IP Phone 8540 telephones	<a href="#">KB 3050590</a>	May 2015
Cumulative update for Lync Phone Edition for Aastra 6721ip and Aastra 6725ip telephones	<a href="#">KB 2954032</a>	April 2014
Cumulative update for Lync Phone Edition for HP 4110 and HP 4120 telephones	<a href="#">KB 2954033</a>	April 2014

PACKAGE NAME	KB NUMBER	RELEASE DATE
Cumulative update for Lync Phone Edition for Polycom CX500, Polycom CX600, and Polycom CX3000 telephones	<a href="#">KB 2954034</a>	April 2014
Cumulative update for Lync Phone Edition for Polycom CX700 and LG-Nortel IP Phone 8540 telephones	<a href="#">KB 2954035</a>	April 2014

### Lync Phone Edition clients on Download Center

PACKAGE NAME	RELEASE DATE
<a href="#">Lync Phone Edition for HP 4110 and HP 4120</a>	April 2017
<a href="#">Lync Phone Edition for Polycom CX500, Polycom CX600 and Polycom CX3000</a>	April 2017
<a href="#">Lync Phone Edition for Polycom CX700 and LG-Nortel IP Phone 8540</a>	December 2015

### Lync Basic 2013 Software

PACKAGE NAME	RELEASE DATE
<a href="#">Lync Basic 2013 (32-bit)</a>	October 2012
<a href="#">Lync Basic 2013 (64-bit)</a>	October 2012

### Lync for Mac 2011 client updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Lync for Mac 2011	<a href="#">KB 3175174</a>	July 2016
Cumulative updates for Lync for Mac 2011	<a href="#">KB 3074981</a>	July 2015

### Lync 2010 client updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Security update for Lync 2010	<a href="#">KB 4025865</a>	September 2017
Security update for Lync 2010	<a href="#">KB 4010732</a>	June 2017
Security update for Lync 2010	<a href="#">KB 4010299</a>	March 2017
Security update for Lync 2010	<a href="#">KB 3188397</a>	October 2016
Security update for Lync 2010	<a href="#">KB 3174301</a>	August 2016

PACKAGE NAME	KB NUMBER	RELEASE DATE
Update for Lync 2010	<a href="#">KB 3171499</a>	June 2016
Security update for Lync 2010	<a href="#">KB 3115871</a>	December 2015
Security update for Lync 2010	<a href="#">KB 3096735</a>	November 2015
Security update for Lync 2010	<a href="#">KB 3081087</a>	September 2015
Cumulative updates for Lync 2010	<a href="#">KB 3072611</a>	July 2015

### Lync 2010 Attendant updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Cumulative update for Lync 2010 Attendant	<a href="#">KB 2842632</a>	July 2013

### Lync 2010 Attendee updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Security update for Lync 2010 Attendee (admin level install)	<a href="#">KB 4025866</a>	September 2017
Security update for Lync 2010 Attendee (admin level install)	<a href="#">KB 4025866</a>	June 2017
Security update for Lync 2010 Attendee (user level install)	<a href="#">KB 4020734</a>	June 2017
Security update for Microsoft Graphics Component on Lync 2010 Attendee (admin level install)	<a href="#">KB 4010301</a>	March 2017
Security update for Lync 2010 Attendee (admin level install)	<a href="#">KB 3188400</a>	October 2016
Description of the cumulative update for the Lync 2010 Attendee - Administrator level installation	<a href="#">KB 3171502</a>	June 2016
Description of the cumulative update for the Lync 2010 Attendee - User level installation	<a href="#">KB 3171496</a>	June 2016
Security update for Lync 2010 Attendee (admin-level installation)	<a href="#">KB 3081089</a>	September 2015
Security update for Lync 2010 Attendee (user-level installation)	<a href="#">KB 3081088</a>	September 2015

### Attendant

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync 2010 Attendant (32 Bit)</a>	November 2010
<a href="#">Lync 2010 Attendant (64 Bit)</a>	November 2010

### Attendee

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync 2010 Attendee - Admin Level Install</a>	April 2013
<a href="#">Lync 2010 Attendee - User Level Install</a>	June 2014

## Related topics

- [Skype for Business Server updates](#)

# Skype for Business Server updates

12/5/2019 • 8 minutes to read

Find and manage updates for [Skype for Business Server 2019](#), [Skype for Business Server 2015](#), [Lync Server 2013](#), and [Lync Server 2010](#) in one place. Use the links on this page to get more information about updates, and then download the updates.

For the latest Skype for Business Online and Office 365 updates, see the [Microsoft 365 Roadmap](#).

## Skype for Business Server 2019 update history

KB 4470124 is the master KB for Skype for Business Server 2019 which has all the historical list of all the Cumulative Update and Hotfixes that have been published.

PACKAGE NAME	KB NUMBER	RELEASE DATE
Skype for Business Server 2019 Cumulative Update 2	<a href="#">KB 4470124</a>	December 2019
Skype for Business Server 2019 Cumulative Update 1 Hotfix 1	<a href="#">KB 4470124</a>	September 2019
Skype for Business Server 2019 Cumulative Update 1	<a href="#">KB 4470124</a>	July 2019

### Skype for Business Server 2019 tools

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">UCMA 6.0 SDK</a>	June 2019
<a href="#">Unified Communications Managed API 5.0 Runtime</a>	June 2018
<a href="#">Skype for Business Server 2019, Management Pack</a>	June 2018

## Skype for Business Server 2015 update history

[KB 3061064](#) contains all Cumulative Updates that have been released.

PACKAGE NAME	KB NUMBER	RELEASE DATE
Skype for Business Server 2015 Cumulative Update 10 Hotfix 1	<a href="#">KB 3061064</a>	August 2019
Skype for Business Server 2015 Cumulative Update 10	<a href="#">KB 3061064</a>	July 2019



<b>PACKAGE NAME</b>	<b>KB NUMBER</b>	<b>RELEASE DATE</b>
Cumulative update 9 for Skype for Business Server 2015, Web Components Server	<a href="#">KB 4487981</a>	May 2019
Cumulative update 8 for Skype for Business Server 2015, Front End Server and Edge Server	<a href="#">KB 4464355</a>	January 2019
Cumulative update 7 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 4340904</a>	July 2018
Cumulative update 6 Hotfix 2 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 4086059</a>	March 2018
Cumulative update 6 Hotfix 1 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 4074701</a>	January 2018
Cumulative update 6 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 4036312</a>	December 2017
Cumulative update 5 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 4012621</a>	May 2017
Cumulative update 4 Hotfix 1 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 3207506</a>	February 2017
Cumulative update 4 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 3199093</a>	November 2017
Cumulative update 3 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 3149227</a>	June 2016
Cumulative update 2 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 3134260</a>	March 2016
Cumulative update 1 for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 3097645</a>	November 2015
Cumulative update for Skype for Business Server 2015, core components	<a href="#">KB 3098601</a>	September 2015
Cumulative update for Skype for Business Server 2015, Front End server and Edge server	<a href="#">KB 3061059</a>	June 2015

## Skype for Business Server 2015 tools

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">UCMA 5.0 SDK</a>	May 2015
<a href="#">Unified Communications Managed API 5.0 Runtime</a>	May 2015
<a href="#">Skype for Business Server 2015, Management Pack</a>	June 2019

## Lync Server 2013 update history

[KB 2809243](#) contains all Cumulative Updates that have been released.

PACKAGE NAME	KB NUMBER	RELEASE DATE
Lync Server 2013 Cumulative Update 10 Hotfix 3	<a href="#">KB 4515509</a>	September 2019
Lync Server 2013 Cumulative Update 10 Hotfix 2	<a href="#">KB 4501392</a>	June 2019
Lync Server 2013 Cumulative Update 10 Hotfix 1	<a href="#">KB 4458772</a>	January 2019
Lync Server 2013 Cumulative Update 10	<a href="#">KB 4295703</a>	July 2018
Lync Server 2013 Cumulative Update 9	<a href="#">KB 4019183</a>	July 2017
Lync Server 2013 Cumulative Update 8 Hotfix 4	<a href="#">KB 4014154</a>	March 2017
Lync Server 2013 Cumulative Update 8 Hotfix 3	<a href="#">KB 3210166</a>	January 2017
Lync Server 2013 Cumulative Update 8 Hotfix 2	<a href="#">KB 3212869</a>	December 2016
Lync Server 2013 Cumulative Update 8 Hotfix 1	<a href="#">KB 3200079</a>	November 2016
Lync Server 2013 Cumulative Update 8	<a href="#">KB 3175336</a>	August 2016
Lync Server 2013 Cumulative update 7	<a href="#">KB 3140581</a>	April 2016
Lync Server 2013 Cumulative Update 6 Hotfix 2	<a href="#">KB 3175338</a>	January 2016
Lync Server 2013 Cumulative Update 6 Hotfix 1	<a href="#">KB 3121213</a>	December 2015
Lync Server 2013 Cumulative Update 6	<a href="#">KB 3081739</a>	September 2015

PACKAGE NAME	KB NUMBER	RELEASE DATE
Lync Server 2013 Cumulative Update 5 Hotfix 10	<a href="#">KB 3064728</a>	July 2015
Lync Server 2013 Cumulative Update 5 Hotfix 9	<a href="#">KB 3051951</a>	May 2015
Lync Server 2013 Cumulative Update 5 Hotfix 8	<a href="#">KB 3031065</a>	February 2015
Lync Server 2013 Cumulative Update 5 Hotfix 7.1	<a href="#">KB 3027553</a>	December 2014
Lync Server 2013 Cumulative Update 5 Hotfix 7	<a href="#">KB 3018232</a>	December 2014
Lync Server 2013 Cumulative Update 5 Hotfix 6	<a href="#">KB 3010028</a>	November 2014
Lync Server 2013 Cumulative Update 5 Hotfix 5	<a href="#">KB 3003358</a>	October 2014
Lync Server 2013 Cumulative Update 5 Hotfix 2	<a href="#">KB 2987511</a>	Sept 2014
Lync Server 2013 Cumulative Update 5	<a href="#">KB 2937305</a>	August 2014
Lync Server 2013 Cumulative Update 4	<a href="#">KB 2905040</a>	January 2014
Lync Server 2013 Cumulative Update 3	<a href="#">KB 881682</a>	October 2013
Lync Server 2013 Cumulative Update 2	<a href="#">KB 2835432</a>	July 2013
Lync Server 2013 Cumulative Update 1	<a href="#">KB 2781550</a>	February 2013

### Lync Server 2013 Dev tools

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Unified Communications Managed API 4.0 Runtime Cumulative Update</a>	July 2013
<a href="#">Lync Server 2013 SDK</a>	February 2013
<a href="#">Lync 2013 SDK</a>	March 2014
<a href="#">Lync Server 2013 Debugging Tools</a>	January 2014
<a href="#">Lync Server 2013 Persistent Chat Server SDK</a>	October 2013
<a href="#">Unified Communications Managed API 4.0 SDK</a>	February 2013

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Unified Communications Managed API 4.0 Runtime</a>	October 2012
<a href="#">UC Enhanced Presence Schemas for Lync Server 2013</a>	October 2012

#### Pre-configured VHDs

The complete topology consists of 7 virtual machines that enable you to fully evaluate the Microsoft Lync 2013, Microsoft Exchange 2013, SharePoint 2013, and UC developer platform APIs (including Microsoft Lync 2013 SDK, Exchange Web Services Managed API 2.0, Microsoft Lync Server 2013 SDK, and Microsoft Unified Communications Managed API 4.0).

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Test Drive - Lync Server 2013 - Part 1 of 3</a>	September 2013
<a href="#">Test Drive - Lync Server 2013 - Part 2 of 3</a>	September 2013
<a href="#">Test Drive - Lync Server 2013 - Part 3 of 3</a>	September 2013

#### Lync 2013 Tools

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync Connectivity Analyzer (32-bit) RETIRED</a>	June 2017
<a href="#">Lync Connectivity Analyzer (64-bit) RETIRED</a>	June 2017
<a href="#">Lync Server 2013 Best Practices Analyzer</a>	October 2012
<a href="#">Lync Server 2013 Capacity Calculator</a>	July 2013
<a href="#">Lync Server 2013 Debugging Tools</a>	January 2014
<a href="#">Lync Server 2013 Management Pack</a>	May 2016
<a href="#">Lync Server 2013 Persistent Chat Resource Kit</a>	July 2013
<a href="#">Lync Server 2013 Planning Tool</a>	July 2013
<a href="#">Lync Server 2013 Resource Kit Tools</a>	January 2014
<a href="#">Lync Server 2013 Stress and Performance Tool</a>	March 2013
<a href="#">Lync Server 2013 Whiteboard Archiving Viewer</a>	February 2013
<a href="#">Lync VDI 2013 plugin (32-bit)</a>	October 2012
<a href="#">Lync VDI 2013 plugin (64-bit)</a>	October 2012
<a href="#">New Office Visio Stencil</a>	July 2016

#### Lync 2013 downloadable documentation

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync Server 2013 Documentation Help File</a>	August 2015

## Lync Server 2010 update history

[KB 2493736](#) contains all Cumulative Updates that have been released.

PACKAGE NAME	KB NUMBER	RELEASE DATE
Lync Server 2010 Cumulative Update 18	<a href="#">KB 2493736</a>	January 2019
Lync Server 2010 Cumulative Update 17	<a href="#">KB 3148801</a>	April 2016
Lync Server 2010 Cumulative Update 16	<a href="#">KB 3057803</a>	May 2015
Lync Server 2010 Cumulative Update 15	<a href="#">KB 3030726</a>	February 2015
Lync Server 2010 Cumulative Update 13	<a href="#">KB 2982385</a> <a href="#">KB 2982388</a>	September 2014
Lync Server 2010 Cumulative Update 12	<a href="#">KB 2957044</a>	April 2014
Lync Server 2010 Cumulative Update 11	<a href="#">KB 2909888</a>	January 2014
Lync Server 2010 Cumulative Update 10	<a href="#">KB 2889610</a>	October 2013
Lync Server 2010 Cumulative Update 9	<a href="#">KB 2860700</a>	July 2013
Lync Server 2010 Cumulative Update 8	<a href="#">KB 2791381</a>	July 2013
Lync Server 2010 Cumulative Update 7	<a href="#">KB 2737915</a>	October 2012
Lync Server 2010 Cumulative Update 6	<a href="#">KB 2701585</a>	June 2012
Lync Server 2010 Cumulative Update 5	<a href="#">KB 2670352</a>	February 2012
Lync Server 2010 Cumulative Update 4	<a href="#">KB 2514980</a>	November 2011
Lync Server 2010 Cumulative Update 3	<a href="#">KB 2571546</a>	July 2011
Lync Server 2010 Cumulative Update 2	<a href="#">KB 2500442</a>	April 2011
Lync Server 2010 Cumulative Update 1	<a href="#">KB 2467775</a>	January 2011

## Group Chat 2010 updates

PACKAGE NAME	KB NUMBER	RELEASE DATE
Cumulative update for Lync Server 2010, Group Chat	<a href="#">KB 2884623</a>	October 2013
Cumulative update for Lync Server 2010, Group Chat Administration Tool	<a href="#">KB 2884631</a>	October 2013
Cumulative update for Lync 2010, Group Chat	<a href="#">KB 2884627</a>	October 2013

## Lync 2010 Dev Tools

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync Server 2010 SDK</a>	November 2010
<a href="#">Lync 2010 SDK</a>	March 2011
<a href="#">Lync Server 2010 Group Chat SDK</a>	June 2012
<a href="#">Unified Communications Managed API 3.0 SDK</a>	May 2016
<a href="#">Speech Platform - Server Runtime Languages (Version 10.2)</a>	September 2010
<a href="#">Unified Communications Enhanced Presence Schemas for Microsoft Lync Server 2010</a>	November 2010

## Lync 2010 Tools

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">IM an Expert for Microsoft Lync Server 2010</a>	March 2012
<a href="#">Lync Server 2010 Best Practices Analyzer</a>	February 2011
<a href="#">Lync Server 2010 Capacity Calculator</a>	February 2012
<a href="#">Lync Server 2010 Planning Tool</a>	February 2011
<a href="#">Lync Server 2010 Resource Kit Tools</a>	May 2012
<a href="#">Lync Server 2010 Stress and Performance Tool</a>	March 2011
<a href="#">Lync Server 2010 Visio Stencil</a>	February 2011
<a href="#">Lync Server 2010 Web Scheduler</a>	April 2011

## Lync 2010 downloadable documentation

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync Server 2010 Documentation Help File</a>	March 2012
<a href="#">Lync Server 2010 Welcome page</a>	October 2012
<a href="#">IM an Expert for Microsoft Lync Server 2010 Documentation</a>	March 2012
<a href="#">Lync 2010 Release Notes.aspx)</a>	January 2011
<a href="#">Lync Server 2010 Release Notes</a>	January 2011
<a href="#">Lync Server 2010 Planning Tool Readme</a>	January 2011
<a href="#">Lync Server 2010 Edge Server Reference Architecture Diagrams</a>	March 2011

### Resource kit (technical reference)

Visit the [Microsoft Lync Server 2010 Resource Kit](#) download site to download book chapters individually OR download a .zip file containing [all 19 chapters of the resource kit](#).

### Group Chat

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">Lync Server 2010 Group Chat</a>	November 2010
<a href="#">Lync Server 2010 Group Chat Admin Tool</a>	November 2010
<a href="#">Lync 2010 Group Chat</a>	November 2010

### Trial Software

PACKAGE NAME/LINK	RELEASE DATE
<a href="#">VHD Test Drive - Lync Server 2010 (Eval) - Part 1 of 2</a>	September 2012
<a href="#">VHD Test Drive - Lync Server 2010 (Eval) - Part 2 of 2</a>	September 2012

## Additional information

Software updates include any update, update rollup, service pack, feature pack, critical update, security update, or hotfix. See [KB 824684](#) for a description of the standard terminology used to describe Microsoft software updates.

## Related topics

- [Install Skype for Business Server 2015](#)
- [Upgrade to Skype for Business Server 2015](#)
- [Latest updates for versions of Skype for Business that use Windows Installer \(MSI\)](#)

# Plan hybrid connectivity between Skype for Business Server and Office 365

9/3/2019 • 9 minutes to read

## Overview

Read this topic to learn how to plan hybrid connectivity between Skype for Business Server and Teams or Skype for Business Online. Setting up hybrid connectivity is the first step in moving your on-premises environment to the cloud.

If you have on-premises Skype for Business users that are also using Teams (side by side), those users do not have the ability to interoperate with Skype for Business users from their Teams client, nor communicate with users in federated organizations, from their Teams client. To gain this functionality in Teams, these users must be moved from Skype for Business on-premises to the cloud, which requires configuring Skype for Business hybrid mode. In addition, for the best experience, these users should be in Teams Only mode, which ensures all incoming calls and chats from any user land in the user's Teams client.

Setting up hybrid connectivity and moving all users to the cloud is also required before you decommission your on-premises Skype for Business deployment. With hybrid connectivity set up, you can choose to move your users to the cloud based on your schedule and business need. With Direct Routing, you can leverage your on-premises voice infrastructure while you move to the cloud and after your migration is complete.

This topic describes the infrastructure and system requirements you'll need to configure hybrid connectivity between your existing on-premises Skype for Business Server deployment and Teams or Skype for Business Online.

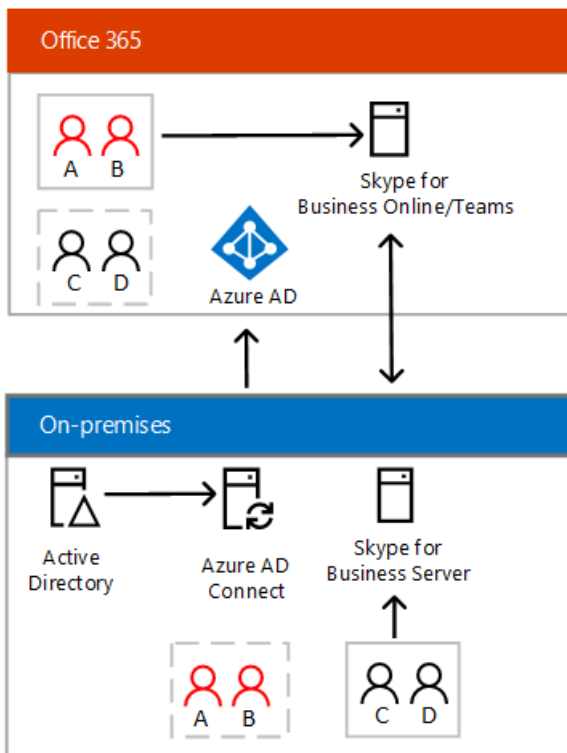
After you have read this topic and are ready to configure hybrid connectivity, see [Configure hybrid connectivity between Skype for Business Server and Office 365](#). The configuration topics provide step-by-step guidance for setting up hybrid connectivity between your on-premises deployment and Teams or Skype for Business Online.

## About Shared SIP Address Space functionality

With hybrid connectivity set up between an on-premises deployment of Skype for Business Server and Teams or Skype for Business Online, you can have some users homed on-premises and some users homed online.

This type of configuration relies on shared SIP address space functionality, and is sometimes referred to as "split domain"--meaning users of a domain, such as contoso.com, are split between using Skype for Business Server on premises and Teams or Skype for Business Online, as shown in the following diagram:





When shared SIP address space is configured:

- Azure Active Directory Connect is used to synchronize your on-premises directory with Office 365.
- Users who are homed on premises interact with on-premises Skype for Business servers.
- Users who are homed online may interact with Skype for Business Online or Teams services.
- Users from both environments can communicate with each other.
- The on-premises Active Directory is authoritative. All users should be created in the on-premises Active Directory first, and then synchronized to Azure AD. Even if you intend for the user to be homed online, you must first create the user in the on-premises environment, and then move the user to online to ensure the user is discoverable by on-premises users.

Before a user can be moved online, the user must be assigned a Skype for Business Online (Plan 2) license. If the user will be using Teams, the user must also be assigned a Teams license (and the Skype for Business license must remain enabled). If your users want to take advantage of additional online features, such as Audio Conferencing or Phone System, you need to assign them the appropriate license in Office 365.

## Infrastructure requirements

To implement hybrid connectivity between your on-premises environment and Office 365 communication services, you need to meet the following infrastructure requirements:

- A single on-premises deployment of Skype for Business Server or Lync Server that is deployed in a supported topology. See [Topology requirements](#) in this topic.
- A Microsoft Office 365 tenant with Skype for Business Online enabled.

### NOTE

You can use only a single tenant for a hybrid configuration with your on-premises deployment.

- Azure Active Directory Connect to synchronize your on-premises directory with Office 365. For more information, see [Azure AD Connect: Accounts and permissions](#).
- Skype for Business Server administrative tools. These are required to move users from on-premises to the cloud. These tools must be installed on a server with access to both on-premises deployment and the internet.

- Online administrative tools. You can use either the Teams admin center or Windows PowerShell to manage Teams and Skype for Business Online. To use PowerShell to manage either Teams or Skype for Business Online, download and install the Skype for Business Online Connector.
- Shared SIP address space must be enabled, and your on-premises deployment must be configured to use Office 365 as a hosting provider. For more information about the steps required to configure hybrid connectivity, see [Configure hybrid connectivity](#).

After you configure hybrid connectivity, you can move users to Teams or Skype for Business Online. For more information, see [Move users from on-premises to Teams](#) and [Move users from on premises to Skype for Business Online](#).

## Server version requirements

To configure your deployment for hybrid with **Teams or Skype for Business Online**, you need to have one of the following supported topologies:

- A Skype for Business Server 2019 deployment with all servers running Skype for Business Server 2019.
- A Skype for Business Server 2015 deployment with all servers running Skype for Business Server 2015.
- A Lync Server 2013 deployment with all servers running Lync Server 2013. However, if hybrid voice connectivity is required, you must use a mixed version topology as noted below.
- A deployment with maximum of 2 different server versions as listed below:
  - Skype for Business Server 2015 and Skype for Business Server 2019
  - Lync Server 2013 and Skype for Business Server 2019
  - Lync Server 2013 and Skype for Business Server 2015

*If hybrid voice is desired in any topology*, both the edge server that is designated as the Federation Edge as well as the pool associated with SIP federation must be running Skype for Business 2015 or later. Users can remain on a Lync 2013 Pool if one exists. For more details, see [Plan Phone System with PSTN Connectivity in Skype for Business Server](#).

The following topologies that include **Lync Server 2010 are supported with Skype for Business Online** for instant messaging and meetings. Topologies that include **Lync Server 2010 are not supported for hybrid voice nor Teams**.

- A mixed Lync Server 2010 and Skype for Business Server 2015 deployment
- A mixed Lync Server 2010 and Lync Server 2013 deployment
- A Lync Server 2010 deployment with all servers running Lync Server 2010 with the latest cumulative updates.

The federation Edge Server and next hop server from the federation Edge Server must be running Lync Server 2010 with the latest cumulative updates. The Skype for Business Server 2015 or Lync Server 2013 Administrative Tools must be installed on at least one server or management workstation.

## Multi-forest support

Microsoft supports the following types of multi-forest hybrid scenarios:

- **Resource forest topology.** In this kind of topology, there is one forest that hosts Skype for Business Server (the resource forest), and there are one or more additional forests that host account identities, which access the Skype for Business Server in the resource forest. In general, users can access Skype for Business functionality in another forest if the following requirements are met:
  - Users are properly synchronized into the forest that hosts Skype for Business. In hybrid configurations, this means that users must be synchronized as disabled user objects.
  - The forest hosting Skype for Business must trust the forest containing the users. For details on

resource forest hybrid scenarios, see [Deploy a resource forest topology for hybrid Skype for Business](#).

- **Multiple deployments of Skype for Business Server in multiple forests.** This configuration can arise as a result of merger and acquisition scenarios, as well as in more complex enterprises. Consolidation of all users from on premises to the cloud in a single Office 365 tenant can be achieved for any organization with multiple Skype for Business deployments, provided that the following key requirements are met:
  - There must be at most one Office 365 tenant involved. Consolidation in scenarios with more than one Office 365 tenant is not supported.
  - At any given time, only one on-premises Skype for Business forest can be in hybrid mode (shared SIP address space). All other on-premises Skype for Business forests must remain fully on premises (and presumably federated with each other). Note that these other on-premises organizations can sync to AAD if desired with [new functionality to disable online SIP domains](#) available as of December 2018.

Customers with deployments of Skype for Business in multiple forests must fully migrate each Skype for Business forest individually into the Office 365 tenant using split-domain (Shared SIP Address Space) functionality, and then disable hybrid with the on-premises deployment, before moving on to migrate the next on-premises Skype for Business deployment. Furthermore, prior to being migrated to the cloud, on-premises users remain in a federated state with any users that are not represented in the same user's on-premises directory. For more details, see [Cloud consolidation for Teams and Skype for Business](#).

## Federation requirements

When configuring hybrid, you must ensure that your on-premises and online environments can federate with each other. The online environment has open federation by default; the on-premises environment often has closed federation by default.

The following requirements must be met to successfully configure a hybrid deployment:

- Domain matching must be configured the same for your on-premises deployment and your Office 365 tenant. If partner discovery is enabled on the on-premises deployment, then open federation must be configured for your online tenant. If partner discovery is not enabled, then closed federation must be configured for your online tenant.
- The Blocked domains list in the on-premises deployment must exactly match the Blocked domains list for your online tenant.
- The Allowed domains list in the on-premises deployment must exactly match the Allowed domains list for your online tenant.
- Federation must be enabled for the external communications for the online tenant.

## Network considerations

The following sections describe considerations for:

- DNS settings
- Firewall considerations

### DNS settings

When creating DNS records for hybrid deployments, all Skype for Business external DNS records should point to the on-premises infrastructure. For details on required DNS records, please refer to [DNS requirements for Skype for Business Server](#).

Additionally, you need to ensure that the DNS resolution described in the following table works in your on-premises deployment. (If you already configured federation for on-premises, then you most likely already have

these.)

DNS RECORD	RESOLVABLE BY	DNS REQUIREMENT
DNS SRV record for _sipfederationtls._tcp.<sipdomain.com> for all supported SIP domains resolving to Access Edge external IP(s)	Edge server(s)	Enable federated communication in a hybrid configuration. The Edge Server needs to know where to route federated traffic for the SIP domain that is split between on premises and online. Must use strict DNS name matching between the domain in the user name and the SRV record.
DNS A record(s) for Edge Web Conferencing Service FQDN, e.g. webcon.contoso.com resolving to Web Conferencing Edge external IP(s)	Internal corporate network connected users' computers	Enable online users to present or view content in on-premises hosted meetings. Content includes PowerPoint files, whiteboards, polls, and shared notes.

Depending on how DNS is configured in your organization, you may need to add these records to the internal hosted DNS zone for the corresponding SIP domain(s) to provide internal DNS resolution to these records.

### Firewall considerations

Computers on your network must be able to perform standard Internet DNS lookups. If these computers can reach standard Internet sites, your network meets this requirement.

Depending on the location of your Microsoft Online Services data center, you must also configure your network firewall devices to accept connections based on wildcard domain names (for example, all traffic from \*.outlook.com). If your organization's firewalls do not support wildcard name configurations, you will have to manually determine the IP address ranges that you would like to allow and the specified ports.

For more information, including details about ports and protocol requirements, see [Office 365 URLs and IP address ranges](#).

# Topology Basics for Skype for Business Server

7/22/2019 • 16 minutes to read

**Summary:** Choose your topology for Skype for Business Server. Learn about server collocation for Skype for Business Server.

Before preparing anything else, you'll want to know you're planning for the right topology for your deployment of Skype for Business Server. The first thing you need to decide is if you're going to have an on-premises deployment of Skype for Business Server, or if you're going to combine this with a Skype for Business Server Online deployment in a Hybrid deployment. Either way, you're going to want to read further, as we'll detail the on-premises topologies here, but the Hybrid details are documented in their own section.

You can also see some example topologies in [Reference topologies for Skype for Business Server](#).

## Sites

In Skype for Business Server, you define sites on your network that contain Skype for Business Server components. A site is a set of computers that is well-connected by a high-speed, low-latency network, such as a single local area network (LAN) or two networks connected by a high-speed fiber optic network. Note that Skype for Business Server sites are a separate concept from Active Directory Domain Services sites and Microsoft Exchange Server sites. Your Skype for Business Server sites do not need to correspond to your Active Directory sites.

Skype for Business Server supports on-premises deployment of one or more sites that can be scaled according to your high availability and location requirements.

Your deployment will have at least one central site (also called a datacenter, this is a datacenter for all the servers located in it), and each central site in your deployment will have one Standard Edition server, or at least one Enterprise Edition Front End pool. You can see the differences in each option below:

- Standard Edition server includes a collocated SQL Server Express database.
- Enterprise Edition Front End pool includes:
  - One or more Front End Servers (Ideally at least three, for scalability), with a maximum of twelve. Load-balancing would be required for more than one server.
  - A separate Back End Server.

You can learn more about the various server roles a little later in this section.

In addition to your central sites, you may also end up having one or more branch sites associated with your central site. They depend on the central site for almost all their functionality, so what are they made up of, exactly?

- Survivable Branch Appliance, which combines a public switched telephone network (PSTN) gateway, with some Skype for Business Server functionality.
- Survivable Branch Server, it's a server running Windows Server that has Skype for Business Server Registrar and Mediation Server software installed.
- Stand-alone PSTN gateway (which isn't part of the Survivable Branch Appliance).
- Stand-alone Mediation Server or stand-alone Mediation Server pool (if you don't want to collocate this role with the Survivable Branch Appliance).

# What's in a Skype for Business Server site?

To get into more detail, a central site can also have:

- Multiple Front End pools, in the same domain or different domains (remember in planning that all the Front End Servers in a Front End pool, along with the Back End Servers for the pool, do have to be in the same domain).
- Multiple Standard Edition servers.
- Office Web Apps Server, which is used with Office Web Apps in Skype for Business Server for sharing and rendering of PowerPoint presentations.
- Edge Server or Edge pool (in a perimeter network). Needed if you want your deployment to support federated partners, public IM connectivity, extensible messaging and presence protocol (XMPP) gateway, and remote user access. More details can be found in the Edge Server Planning documentation.
- Persistent Chat Server. Useful if you want users to be able to take part in multiparty, topic-based conversations that persist over time. There's more information at the Planning for Persistent Chat Server topic.
- Monitoring. Used to support data collection for audio/video (A/V) Quality of Experience (QoE) and call detail recording (CDR) for Enterprise Voice and A/V conferences in your deployment. We discuss it in detail at the Planning for Monitoring topic.
- Director or Director pool. Not required, but useful if you want to improve resiliency and enable redirection of Skype for Business user requests to the user's home pool. If you want to deploy Directors, a maximum of 10 per pool is supported. If this is something you need, definitely continue reading at the Planning for Directors topic.
- Reverse proxy. This isn't a Skype for Business Server component, but if you want to support the sharing of web content for federated users, if you intend to support Mobility traffic, if your remote users want to use the address book, join meetings, and so on, this is something you'll want to have in your environment. There's a Setting up Reverse proxy server topic you can check out for more details, when you're ready.

Additional information on collocation for these servers can be found below.

All the Front End pools and Standard Edition servers deployed at your central site share the following, assuming you've deployed them:

Director or Director pool	Stand-alone Mediation Server or Mediation Server pool	Office Web Apps Server
Edge Server or Edge pool	Persistent Chat Server or Persistent Chat Server pool	Monitoring

Where is Exchange Unified Messaging (UM) Server in this list? Well, you can certainly use it with Skype for Business Server if you want to integrate with Exchange UM, but it's not a component of the Skype for Business Server site, so we're not mentioning it here.

You may be planning to have multiple central site, and if that's so, they can share the following servers and roles, if they're deployed on your central site:

Stand-alone Mediation Server or Mediation Server pool	Edge Server or Edge pool
---	--------------------------

Persistent Chat Server or Persistent Chat Server pool	Monitoring
---	------------

Just like the last list, we aren't including the Exchange UM Server here because it's not part of the Skype for Business Server deployment, but it falls into the same category here, too.

There are some other components and options that go into deployments, of course.

Firewalls	PSTN gateways (if you deploy Enterprise Voice)	Exchange UM Server (if you want to integrate with Exchange UM)	DNS load balancing
Hardware load balancers	SQL Server databases	File shares	

## Server roles

Each server running Skype for Business Server runs one or more server roles. A server role is a defined set of Skype for Business Server functionalities provided by that server. You don't need to deploy all available server roles in your network. Install only the server roles that contain the functionality that you want.

For most server roles, for scalability and high availability you can deploy pools of multiple servers all running the same server role. Each server in a pool must run an identical server role or roles. For most types of pools in Skype for Business Server, you must deploy a load balancer to spread traffic between the various servers in the pool. Skype for Business Server supports both Domain Name System (DNS) load balancing and hardware load balancers.

### Front End Server and Back End Server

In Skype for Business Server Enterprise Edition, the Front End Server is the core server role, and runs many basic Skype for Business Server functions. The Front End Server, along with the Back End Servers, are the only server roles required to be in any Skype for Business Server Enterprise Edition deployment.

A Front End pool is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. A pool of multiple servers running the same role provides scalability and failover capability.

The Front End Server includes the following:

- User authentication and registration.
- Presence information and contact card exchange.
- Address book services and distribution list expansion.
- IM functionality, including multiparty IM conferences.
- Web conferencing, PSTN Dial-in conferencing and A/V conferencing (if deployed).
- Application hosting, for both applications included with Skype for Business Server (for example, Conferencing Attendant and Response Group application), and third-party applications.
- Optionally, Monitoring, to collect usage information in the form of call detail records (CDRs) and call error records (CERs). This information provides metrics about the quality of the media (audio and video) traversing your network for both Enterprise Voice calls and A/V conferences.
- Web components to supported web-based tasks such as web scheduler and join launcher.

- Optionally, Archiving, to archive IM communications and meeting content for compliance reasons. For details, see [Planning for Archiving](#) in the Planning documentation.

In Lync Server 2010 and prior versions, Monitoring and Archiving were separate server roles, not collocated on Front End Server.

- Optionally, if Persistent chat is enabled, Persistent Chat Web Services for Chat Room Management and Persistent Chat Web Services for File Upload/Download.

Front End Pools are also the primary store for user and conference data. Information about each user is replicated among three Front End Servers in the pool, and backed up on the Back End Servers.

Additionally, one Front End Server in the deployment also runs the Central Management Server, which manages and deploys basic configuration data to all servers running Skype for Business Server. The Central Management Server also provides Lync Server Management Shell and file transfer capabilities.

The Back End Servers are database servers running Microsoft SQL Server that provide the database services for the Front End pool. The Back End Servers serve as backup stores for the pool's user and conference data, and are the primary stores for other databases such as the Response Group database. You can have a single Back End Server, but [Back End Server high availability in Skype for Business Server](#) is recommended for failover. Back End Servers do not run any Skype for Business Server software.

#### **IMPORTANT**

We do not recommend collocating Skype for Business Server databases with other databases. If you do so, availability and performance may be affected.

#### **NOTE**

SQL Mirroring is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering methods are preferred with Skype for Business Server 2019.

Information stored in the Back End Server databases includes presence information, users' Contacts lists, conferencing data, including persistent data about the state of all current conferences, and conference scheduling data.

### **Edge Server**

Edge Server enables your users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization's own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Skype for Business Server deployment.

Deploying Edge Server also enables mobility services, which supports Lync functionality on mobile devices. Users can use supported Apple iOS, Android, Windows Phone, or Nokia mobile devices to perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed calls. The mobility feature also supports push notifications for mobile devices that do not support applications running in the background. A push notification is a notification that is sent to a mobile device about an event that occurs while a mobile application is inactive.

Edge Servers also include a fully-integrated Extensible Messaging and Presence Protocol (XMPP) proxy, with an XMPP gateway included on Front End Servers. You can configure these XMPP components to enable your Skype for Business Server users to add contacts from XMPP-based partners for instant messaging and presence.



**NOTE**

XMPP Gateways and proxies are available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See [Migrating XMPP federation](#) for more information.

**Mediation Server**

Mediation Server is a necessary component for implementing Enterprise Voice, Call Via Work, and dial-in conferencing. Mediation Server translates signaling, and, in some configurations, media between your internal Skype for Business Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. You can run Mediation Server collocated on the same server as Front End Server, or separated into a stand-alone Mediation Server pool.

For details, see [Mediation Server component in Skype for Business Server](#).

**Video Interop Server**

Video Interop Server is a new role as of Skype for Business Server 2015. It enables you to integrate your Skype for Business Server deployment with certain third-party VTC (Video Teleconferencing System) solutions. A VIS acts as an intermediary between a 3rd party teleconference system and a Skype for Business Server deployment. For this release, VIS is focused on interoperability with Cisco/Tandberg video systems.

For details, see [Plan for Video Interop Server in Skype for Business Server](#).

**Director**

Directors can authenticate Skype for Business Server user requests, but they do not home user accounts or provide presence or conferencing services. Directors are most useful to enhance security in deployments that enable external user access. The Director can authenticate requests before sending them on to internal servers. In the case of a denial-of-service attack, the attack ends with the Director and does not reach the Front End servers.

**Persistent Chat Server Roles****NOTE**

Persistent chat is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The same functionality is available in Teams. For more information, see [Getting started with your Microsoft Teams upgrade](#). If you need to use Persistent chat, your choices are to either migrate users requiring this functionality to Teams, or to continue using Skype for Business Server 2015.

Persistent chat enables users to participate in multiparty, topic-based conversations that persist over time. The Persistent Chat Front End Server runs the persistent chat service. The Persistent Chat Back End Server stores the chat history data, and information about categories and chat rooms. The optional Persistent Chat Compliance Back End Server can store the chat content and compliance events for the purpose of compliance.

Servers running Skype for Business Server Standard Edition can also run Persistent chat collocated on the same server. You cannot collocate the Persistent Chat Front End Server with Enterprise Edition Front End Server.

For details, see [Plan for Persistent Chat Server in Skype for Business Server 2015](#).

## High availability and disaster recovery support

Skype for Business Server provides high availability by server redundancy via pooling. If a server running a certain server role fails, the other servers in the pool running the same role take the load of that server. This applies to Front End Servers, Edge Servers, Mediation Servers, and Directors.

Skype for Business Server also provides disaster recovery measures by enabling pool pairing. If you deploy this topology, you will designate pairs of Front End pools, with each pool in a pair located in a separate data center,

and in a separate geographical area. If one pool or site goes down, you can redirect the users of that pool to use the other pool in the pair, with minimal interruption of service.

Skype for Business Server also supports several options for Back End Server high availability. These include the following:

- Database mirroring
- AlwaysOn Availability Groups
- AlwaysOn Failover Cluster Instances (FCI)
- SQL failover clustering

For details about pool pairing and Back End Server high availability, see [Plan for high availability and disaster recovery in Skype for Business Server](#).

## Server collocation in Skype for Business Server

We've used the term collocate already, but what does this mean? Skype for Business Server allows you to locate some server roles and features on the same server, which is collocation, or on different servers, but it can be confusing when you're starting out, and whether you're doing a Standard Edition or Enterprise Edition server deployment (they each come with their own rules). To help with your planning, we're including server collocation in Standard Edition server deployments and Enterprise Edition Front End pool deployments (in most cases this information is identical, and where it's different, it's called out specifically).

### Collocation of server roles

The Standard Edition server has the following role collocated (additional configuration is required though), while in the Enterprise Edition Front End pool, this role can be collocated, or deployed to a separate server:

- Mediation

These server roles must each be deployed on a separate server:

- Director
- Edge
- Video Interop Server
- Office Web Apps

### Databases

This is the area with real differences between Standard Edition server deployments and Enterprise Edition server pool deployments, so we'll have two sections below, followed by some additional rules for both.

#### Standard

Since SQL Server Express is collocated on the Standard Edition server, and can't be moved, this is pretty straightforward. Furthermore, if you deploy Persistent Chat Server on a Standard Edition server, you're also able to collocate the Persistent Chat and the Persistent Chat compliance database on the Standard Edition server too, but you don't have to.

#### NOTE

Persistent chat is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The same functionality is available in Teams. For more information, see [Getting started with your Microsoft Teams upgrade](#). If you need to use Persistent chat, your choices are to either migrate users requiring this functionality to Teams, or to continue using Skype for Business Server 2015.

These can't be collocated on the Standard Edition server, but can go on a single database server of their own:

- Monitoring database
- Archiving database
- Any back-end database for an Enterprise Edition Front End pool

#### **Enterprise**

The following databases can be collocated on the same back end SQL Server:

- Back End database
- Monitoring database
- Archiving database
- Persistent Chat database
- Persistent Chat compliance database

#### **Both**

Now, there are some additional rules to follow when collocating Skype for Business Server databases in a single SQL instance, or in multiple SQL instances in the same SQL Server database:

- Each SQL instance can only contain a single back end database for an Enterprise Edition Front End pool, a single Monitoring database, a single Archiving database, a single Persistent Chat database, and a single Persistent Chat compliance database.
- The database server can't support more than one Enterprise Edition Front End pool, one server running Archiving, one server running Monitoring, a single Persistent Chat database, and a single Persistent Chat compliance database, but it can support one of each, regardless of whether the databases use the same instance of SQL Server or separate instances of SQL Server.

#### **NOTE**

Persistent chat is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The same functionality is available in Teams. For more information, see [Getting started with your Microsoft Teams upgrade](#). If you need to use Persistent chat, your choices are to either migrate users requiring this functionality to Teams, or to continue using Skype for Business Server 2015.

#### **File shares**

The file share can be on a separate server, or you can collocate it on the same server as any or all of the following:

- Database server, including the Back End Server of an Enterprise Edition Front End pool
- Monitoring database
- Archiving database
- Persistent Chat database
- Persistent Chat compliance database

#### **Caution**

Note that while you can collocate the file share on these servers, it's vital to note that we don't recommend it. If you're collocating the file share with any other server role, please make sure you're monitoring for disk space and performance issues on a regular basis.

#### **Keep in mind**

- You can't collocate a reverse proxy server, which isn't a Skype for Business Server component, and may not even be in your topology. You'll need a reverse proxy if you want to support sharing of web content for federated users, among many other things. If you need to, go ahead and implement reverse proxy support for Skype for Business Server by configuring an existing reverse proxy server that's already in your organization that's being used by other applications.
- You can't collocate any Exchange UM component or SharePoint Server component with any Skype for Business Server role.

## See also

[Reference topologies for Skype for Business Server](#)

# Reference topologies for Skype for Business Server

9/18/2019 • 14 minutes to read

Reference topologies for Skype for Business Server, including diagrams and decisions to make for large, medium, and small organizations.

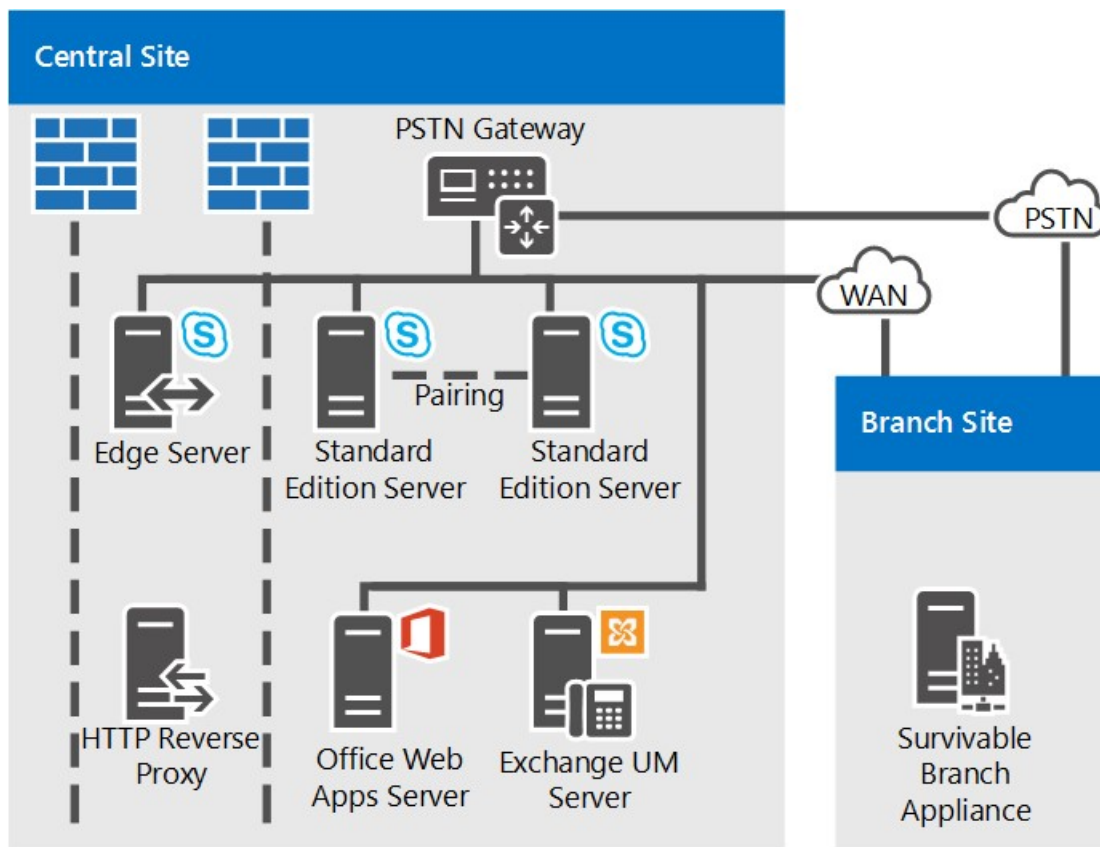
The best Skype for Business Server topology for you depends on your organization's size, the workloads you want to deploy, and your preferences for high availability versus cost of investment.

This section outlines three sample reference topologies, including the reasoning behind many of the decisions that factored into each topology.

## Reference topology for a small organization

The reference topology for small organizations shows how you can deploy a robust, highly available solution by deploying only three servers running Skype for Business Server.

### Reference topology for small organizations



- **Pair of Standard Edition Servers Deployed** This organization has 4,000 users at their central site. They have deployed two Standard Edition servers and paired them together to enable high availability and disaster recovery. Each server homes 2,000 users, but information about all users is synchronized between the two servers. If one goes down, an administrator can fail over those users to be served by the other server, with a minimum of disruption to users. For more information about high availability and disaster recovery features in Skype for Business Server, see [Plan for high availability and disaster recovery in Skype for Business Server](#).
- **Edge Server deployment is recommended.** Although deploying an Edge Server is not required for internal IM, presence and conferencing, we recommend it even for small deployments. You can maximize

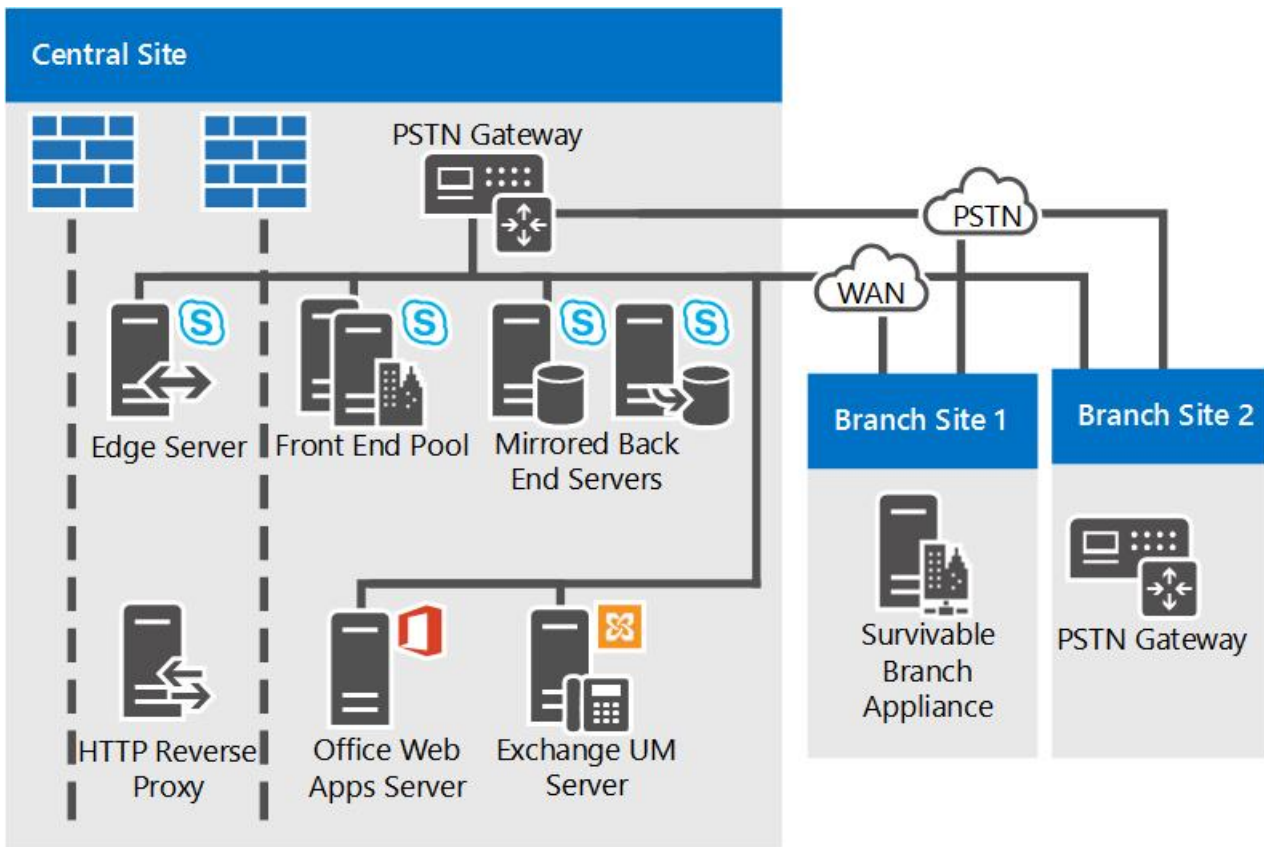
your Skype for Business Server investment by deploying an Edge Server to provide service to users currently outside your organization's firewalls. The benefits include the following:

- Your organization's own users can use Skype for Business Server functionality, if they are working from home or are out on the road.
- Your users can invite outside users to participate in meetings.
- If you have a partner, vendor or customer organization that also uses Skype for Business Server, you can form a federated relationship with that organization. Your Skype for Business Server deployment would then recognize users from that federated organization, leading to better collaboration.
- Your users can exchange instant messages with users of some public IM services.
- **Branch site survivability.** This organization is running a pilot program of the Enterprise Voice feature of Skype for Business Server. Some users are using Skype for Business Server as their sole voice solution. Some of these Enterprise Voice pilot users are located at the branch site. The branch site does not have a reliable wide area network (WAN) link to the central site, so a Survivable Branch Appliance is deployed there. With this deployed, if the WAN link goes down, users at the branch site can still make and receive calls (both calls within the organization and PSTN calls), have voice mail functionality, and communicate with two-party instant messaging (IM). Users can also be authenticated when the WAN link is unavailable as well. For more information, see [Plan for Enterprise Voice resiliency in Skype for Business Server](#).
- **Exchange UM deployment.** This reference topology includes an Exchange Unified Messaging (UM) Server, which runs Microsoft Exchange Server, not Skype for Business Server.
- **Office Web Apps Server.** We recommend deploying an Office Web Apps Server or Office Web Apps Server farm in every organization that uses web conferencing. Office Web Apps Server makes it possible for PowerPoint slides to be presented in web conferences..

## Reference topology for a medium organization

The reference topology with high availability and a single data center is designed for a small-to-medium size organization with one central site. The exact topology in the following diagram is for an organization of 20,000 users.

### Reference topology for medium organizations



- Accommodate more users by adding more Front End Servers.** The exact topology in this diagram has three Front End Servers to provide support for 20,000 users. If you have a single central site and more users, you can simply add more Front End Servers to the pool. The maximum number of users per pool is 80,000, with twelve Front End Servers.

However, the single site topology can support even more users by adding another Front End pool to the site.

- Disaster Recovery could be added.** For this organization, high availability for their Skype for Business Server services is a necessary feature, but disaster recovery is not. The pool of Front End Servers they have deployed provides high availability.

If they wanted to add disaster recovery ability, they could consider establishing another datacenter and adding another Front End pool there, and pairing it with the Front End pool in their current datacenter. Then, if there was a disaster affecting their primary pool, the administrators could fail over users to the backup pool.

- Back End Servers are mirrored** To provide more high availability for basic user features, the organization has deployed a mirrored pair of Back End Servers for each Front End pool.
- Monitoring Server database options.** This organization has deployed Monitoring to ensure the quality of Enterprise Voice calls and A/V conferences. Monitoring is deployed on every Front End Server, and the Monitoring database is collocated with the Back End Servers. We also support topologies in which the Monitoring database is located on a separate server.
- Edge Server high availability** In this example organization with 20,000 users, just one Edge Server would be sufficient for performance. However, they have deployed a pool of two Edge Servers deployed to provide high availability.
- Branch site deployment options.** The organization in this topology has Enterprise Voice deployed as their voice solution. Branch Site 1 does not have a resilient wide area network (WAN) link to the central site, so it has a Survivable Branch Appliance deployed to maintain many Skype for Business Server features in case the WAN link to the central site goes down. Branch Site 2 however has a resilient WAN link, so only a

public switched telephone network (PSTN) gateway is needed. The PSTN gateway deployed there supports media bypass, so no Mediation Server is needed at Branch Site 2. For more information, see [Plan for Enterprise Voice resiliency in Skype for Business Server](#).

- **DNS load balancing.** The Front End pool and Edge Server pool, have DNS load balancing for SIP traffic deployed. This eliminates the need for hardware load balancers for the Edge Servers, and significantly lessens the setup and maintenance of the hardware load balancers for the other pools, as the hardware load balancers are needed only for HTTP traffic. For more information, see [DNS load balancing](#).
- **Exchange UM deployment.** This reference topology includes an Exchange Unified Messaging (UM) Server, which runs Microsoft Exchange Server, not Skype for Business Server.
- **Office Web Apps Server.** We recommend deploying an Office Web Apps Server or Office Web Apps Server farm in every organization that uses web conferencing. Office Web Apps Server makes it possible for Powerpoint slides to be presented in web conferences.
- **Directors could be added.** If this organization wanted to help to increase security against denial of service attacks, it could also deploy a pool of Directors. A Director is a separate, optional server role in Skype for Business Server that does not home user accounts, or provide presence or conferencing services. It serves as an internal next hop server to which an Edge Server routes inbound SIP traffic destined for internal servers. The Director pre-authenticates inbound requests and redirects them to the user's home pool or server. Pre-authentication at the Director allows for dropping of requests from user accounts unknown to the deployment. A Director helps insulate Front End Servers from malicious traffic such as denial-of-service (DoS) attacks. If the network is flooded with invalid external traffic in such an attack, the traffic ends at the Director.
- **System Center Operations Manager is recommended.** We recommend that you monitor the health of your Skype for Business Server deployment to help ensure service availability for end-users. You can use the System Center Operations Manager Management Pack for Skype for Business that is available as a free download from Microsoft. With the Skype for Business Management Pack, you can proactively get real-time alerts when issues occur, run synthetic transactions to test end-to-end Skype for Business functionality, get reports for service availability, and so on. This helps you to proactively respond to issues with your deployment before end-users experience them.

## Reference topology for a large organization

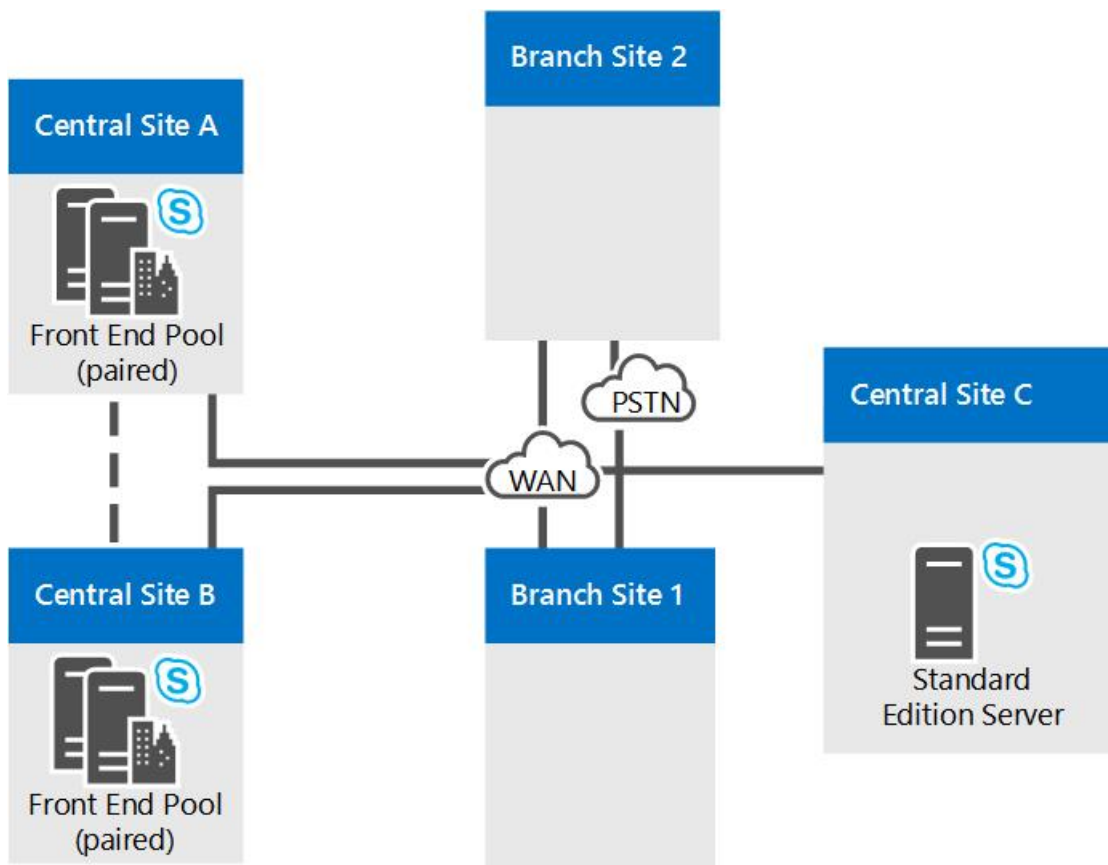
The reference topology for a large organization with multiple data centers support is for any size of organization with more than one central site. The exact topology in the following diagram is for an organization of 50,000 users, with 20,000 users at Central Site A, 20,000 at Central Site B, and a total of 10,000 at Central Site C and branch sites. The type of topology shown in this diagram can accommodate organizations with any number of users.

In addition to the high availability provided by pools of Front End Servers, this topology adds disaster recovery support. The Front End pools at Central Sites A and B are paired together. If one of these pools goes down, the administrator can shift the services for the affected users to the paired pool at the unaffected site.

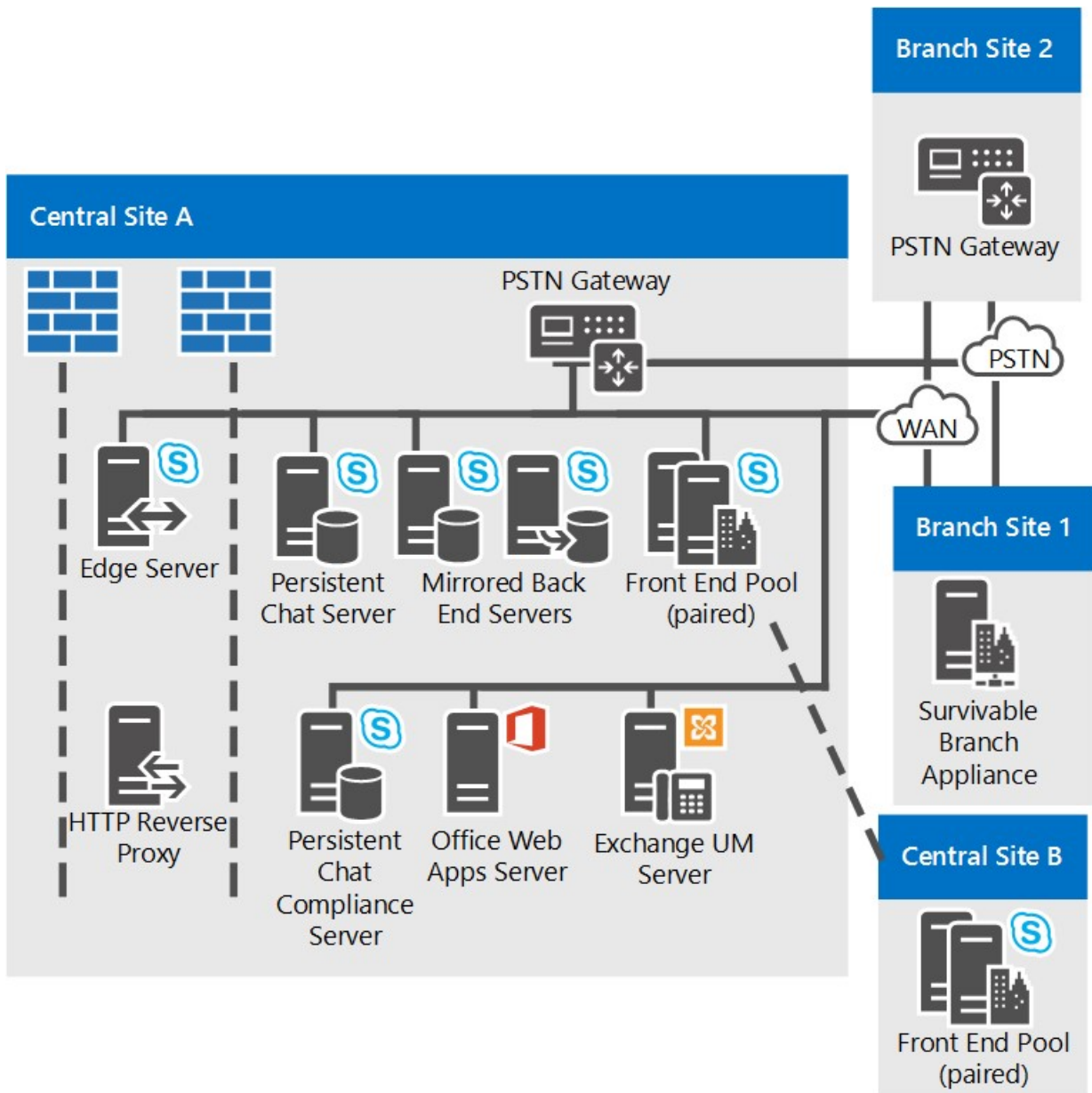
This topology is shown in multiple diagrams, with an overview first followed by detailed views of the central sites.

### Overview of the reference topology for large organizations with multiple data centers

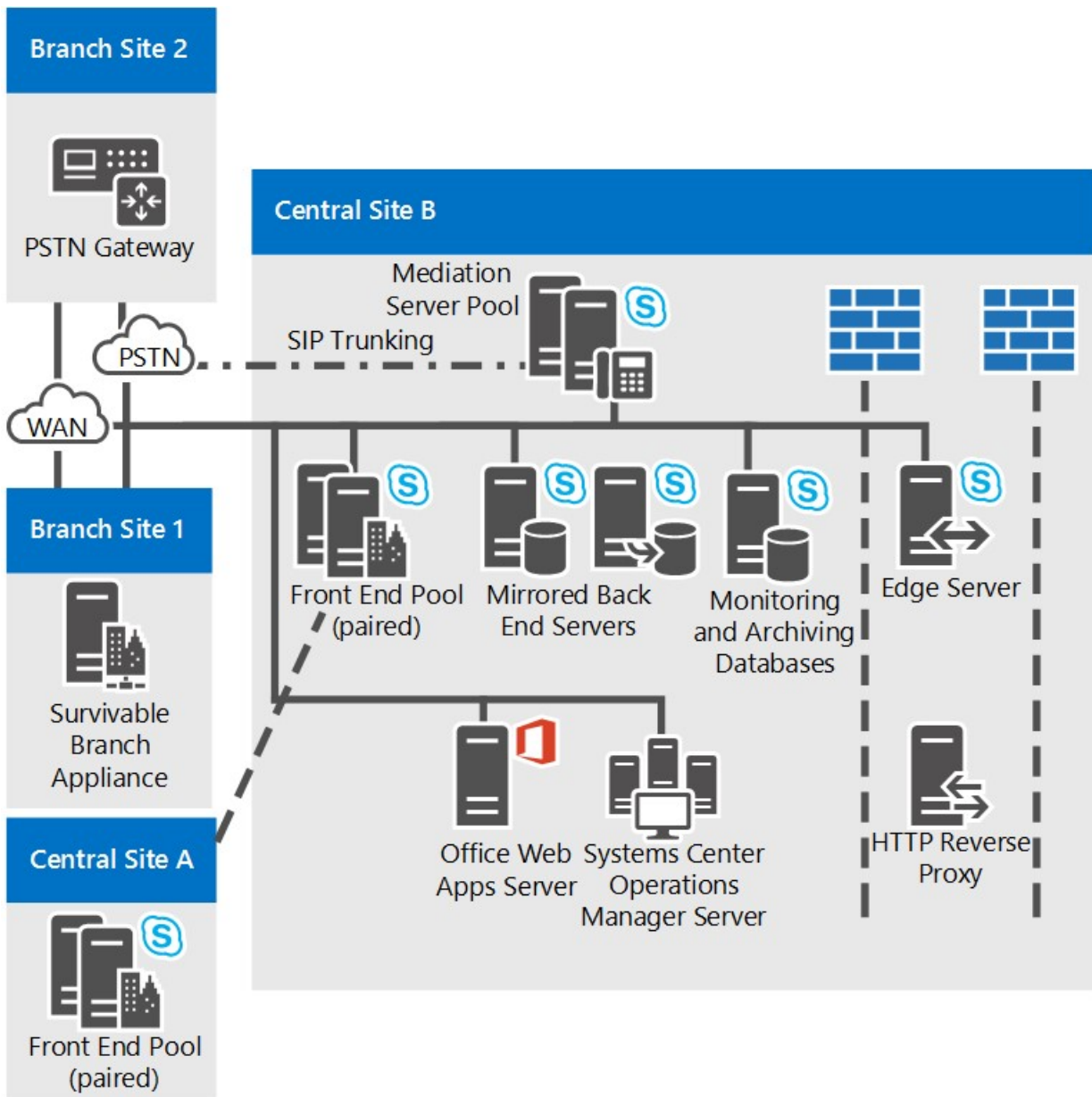




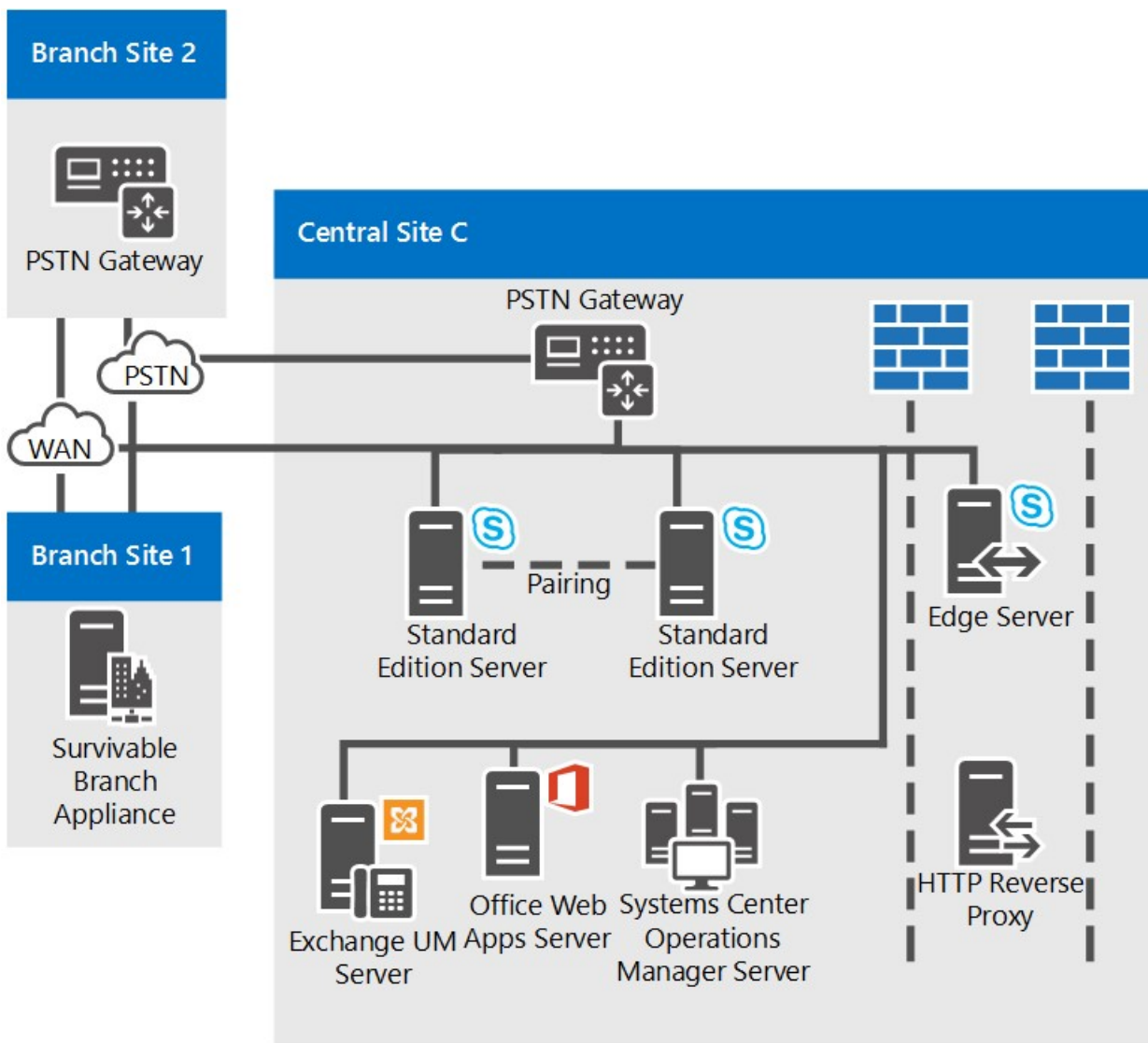
**Reference topology for large organizations: Detailed view of Central Site A**



Reference topology for large organizations: Detailed view of Central Site B



**Reference topology for large organizations: Detailed view of Central Site C**



- Front End pools Are Paired to Enable Disaster Recovery.** The Front End pools at Site A and Site B are paired with each other, to provide disaster recovery support. If the pool at one site fails, the administrator can fail over the users from that site to the paired Front End pool at the other site, with a minimum of service interruption for users. Each of these two Front End pools has six servers, which is enough for all 40,000 users in both pools in case of failover. For more information, see [Plan for high availability and disaster recovery in Skype for Business Server](#).
- Back End Servers are mirrored** To provide more high availability for basic user features, the organization has deployed a mirrored pair of Back End Servers for each Front End pool. This is an optional topology, and you could choose to deploy a single Back End Server instead. SQL clustering and AlwaysOn Availability groups are also supported. For more information, see [Back End Server high availability in Skype for Business Server](#).
- Using Standard Edition server at a branch site.** This organization considers Site C as a branch site because it has only 600 employees. However, the users there have many A/V conferences among themselves. If it was deployed in Skype for Business Server as a branch site, the media for these conferences would run across the wide area network (WAN) to and from a central site that has a Front End Server deployed. To avoid this potential bandwidth load, they have installed a pair of Standard Edition servers at this site, which will host these conferences. And because Standard Edition servers are installed there, Skype for Business Server by definition considers it a central site, and it is treated as such in Topology Builder and the Planning Tool.

Just one Standard Edition server would be enough for performance here, but the organization has deployed two and paired them together to provide high availability in case one server goes down.

Although Site C is considered a central site, you do not have to deploy Edge Servers there. In this example, Site C will use the Edge Servers deployed at Site A.

- **Monitoring and Archiving** This organization has deployed both Monitoring and Archiving. When you deploy Monitoring or Archiving, it runs on every Front End Server. The databases for these features can be collocated with the Back End Database, or located on a separate server. This organization has located these databases on a server separate from the Back End Servers, in Central Site B. The databases here receive Monitoring and Archiving data from the Front End Servers in all sites.
- **Branch site deployment options.** This organization actually has over 50 branch sites, only two of which are shown in the detailed diagrams. Branch Site 1 does not have a resilient WAN link to the central site, so they have Survivable Branch Appliances deployed to provide telephone service in case the WAN link to the central site goes down. Branch Site 2 however has a resilient WAN link, so it needs only a public switched telephone network (PSTN) gateway. The PSTN gateway deployed there supports media bypass, so no Mediation Server is needed at Branch Site 2. For details about deciding what to install at a branch site, see [Plan for Enterprise Voice resiliency in Skype for Business Server](#).
- **SIP trunking and Mediation Server.** Notice that at Central Site B, Mediation Server is not collocated with the Front End Servers. This is because stand-alone Mediation Server is recommended for sites that use SIP trunking. In most other instances, we recommend you collocate Mediation Server with Front End Server. For details about Mediation Server topologies, see [Components and Topologies for Mediation Server](#) in the Planning documentation.
- **Persistent Chat is Deployed.** This organization has deployed the servers necessary to enable Persistent Chat. It has deployed multiple Persistent Chat Front End Servers to both handle the load for the number of users in the pool, and to provide high availability. It has also deployed Compliance for Persistent Chat, and located the Persistent Chat Store and the Persistent Chat Compliance Store on separate servers. These stores could be collocated, and can even be collocated with the Back End Server, but this organization has chosen to separate them to provide better performance.

#### NOTE

Persistent chat is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The same functionality is available in Teams. For more information, see [Getting started with your Microsoft Teams upgrade](#). If you need to use Persistent chat, your choices are to either migrate users requiring this functionality to Teams, or to continue using Skype for Business Server 2015.

- **DNS load balancing.** The Front End pool and Edge Server pool use DNS load balancing. This eliminates the need for hardware load balancers for the internal interface of the Edge Servers, and significantly decreases the amount of time you have to spend on the setup and maintenance of the hardware load balancers for the other pools, as the hardware load balancers are needed only for HTTP traffic. For more information, see ([../plan-your-deployment/network-requirements/load-balancing.md#BKMK\\_DNSLoadBalancing](#)).
- **Exchange UM deployment.** Skype for Business Server works with both on-premises deployments of Exchange Unified Messaging (UM) and hosted Exchange UM. Central Site A includes an Exchange Unified Messaging (UM) Server, which runs Microsoft Exchange Server, not Skype for Business Server. The Exchange UM functionality for Skype for Business Server runs on the Front End pool.

Central Site B uses hosted Exchange, so the Exchange UM Server functionality is also hosted.

For details about Exchange UM, see [On-Premises Exchange Unified Messaging Integration](#) and [Hosted Exchange Unified Messaging Integration](#) in the Planning documentation.

- **Office Web Apps Server.** We recommend deploying an Office Web Apps Server or Office Web Apps Server farm in every organization that uses web conferencing. You could deploy a single Office Web Apps

Server farm in one site which serves traffic from all sites, or deploy it in each site. Office Web Apps Server makes it possible for Powerpoint slides to be presented in web conferences.

- **Directors could be added.** If this organization wanted to increase security against denial of service attacks, it could also deploy a pool of Directors. A Director is a separate, optional server role in Skype for Business Server that does not home user accounts, or provide presence or conferencing services. It serves as an internal next hop server to which an Edge Server routes inbound SIP traffic destined for internal servers. The Director pre-authenticates inbound requests and redirects them to the user's home pool or server. Pre-authentication at the Director allows for dropping of requests from user accounts unknown to the deployment. A Director helps insulate Front End Servers from malicious traffic such as denial-of-service (DoS) attacks. If the network is flooded with invalid external traffic in such an attack, the traffic ends at the Director.
- **System Center Operations Manager is recommended.** We recommend that you monitor the health of your Skype for Business Server deployment to help ensure service availability for end-users. You can use the System Center Operations Manager Management Pack for Skype for Business that is available as a free download from Microsoft. With the Skype for Business Management Pack, you can proactively get real-time alerts when issues occur, run synthetic transactions to test end-to-end Skype for Business functionality, get reports for service availability, and so on. This helps you to proactively respond to issues with your deployment before end-users experience them.

# System requirements for Skype for Business Server 2019

10/9/2019 • 30 minutes to read

**Summary:** Prepare to install Skype for Business Server 2019 with this topic. Hardware, OS, software, databases, certificates, Active Directory, DNS, and fileshares are covered here. All the system requirements and recommendations are here to help ensure a successful install and deployment of your server farm.

As you might expect, there are some preparations to make before you begin deploying Skype for Business Server 2019. This article will walk you through planning for the following:

- [Hardware](#)
- [Operating systems](#)
- [Software](#)
- [Back end SQL databases](#)
- [Active Directory](#)
- [Domain Name System \(DNS\)](#)
- [Certificates](#)
- [File Share](#)

## Hardware for Skype for Business Server 2019

After you have your topology down (and if you don't, you can check out the [Topology Basics for Skype for Business Server 2019](#) topic), it's time to think about servers. Skype for Business Server 2019 servers require 64-bit hardware. Our recommendations for hardware are below. These aren't requirements, but they reflect the requirements necessary for optimal performance. We have capacity planning documentation that will help you determine if you need more than this, depending on your circumstances.

Recommended hardware for Standard Edition servers:

HARDWARE COMPONENT	RECOMMENDED
CPU	Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher. Intel Itanium processors are not supported for Skype for Business Server 2019 roles.
Memory	32 gigabytes (GB).
Disk	EITHER: <ul style="list-style-type: none"><li>• 8 or more 10000 RPM hard disk drives with at least 72 GB free disk space (two of the disks using RAID 1 and 6 using RAID 10).</li></ul> OR <ul style="list-style-type: none"><li>• Solid state drives (SSDs) able to provide the same free space and similar performance to 8 10000 RPM mechanical disk drives.</li></ul>

HARDWARE COMPONENT	RECOMMENDED
Network	<p>1 dual-port network adapter, 1 Gbps or higher (2 network adapters can be used, but they need to be teamed with a single MAC address and a single IP address).</p> <p>Dual or multi-homed configurations are <b>not</b> supported for Front End Servers, Back End Servers, and Standard Edition servers.</p> <p>As long as they are not exposed to the operating system and are being used to monitor and manage server hardware, you can have out-of-band management systems, such as DRAC or ILO. This scenario doesn't constitute a multi-homed server, and it is supported.</p>

Recommended hardware for Front End Servers and Back End Servers:

HARDWARE COMPONENT	RECOMMENDED
CPU	<p>Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher.</p> <p>Intel Itanium processors are not supported for Skype for Business Server 2019 roles.</p>
Memory	64 gigabytes (GB).
Disk	<p>EITHER:</p> <ul style="list-style-type: none"> <li>8 or more 10000 RPM hard disk drives with at least 72 GB free disk space (two of the disks using RAID 1 and 6 using RAID 10).</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>Solid state drives (SSDs) able to provide the same free space and similar performance to 8 10000 RPM mechanical disk drives.</li> </ul>
Network	<p>1 dual-port network adapter, 1 Gbps or higher (2 network adapters can be used, but they need to be teamed with a single MAC address and a single IP address).</p> <p>Dual or multi-homed configurations are <b>not</b> supported for Front End Servers, Back End Servers, and Standard Edition servers.</p> <p>As long as they are not exposed to the operating system and are being used to monitor and manage server hardware, you can have out-of-band management systems, such as DRAC or ILO. This scenario doesn't constitute a multi-homed server, and it is supported.</p>

Recommended hardware for Edge Servers, standalone Mediation Servers, and Directors:

HARDWARE COMPONENT	RECOMMENDED
CPU	<p>Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher.</p> <p>Intel Itanium processors are not supported for Skype for Business Server 2019 roles.</p>
Memory	32 gigabytes.



HARDWARE COMPONENT	RECOMMENDED
Disk	EITHER: <ul style="list-style-type: none"> <li>• 4 or more 10000 RPM hard disk drives with at least 72 GB free disk space (the disks should be in a 2x RAID 1 configuration).</li> </ul> OR <ul style="list-style-type: none"> <li>• Solid state drives (SSDs) able to provide the same free space and similar performance to 4 10000 RPM mechanical disk drives.</li> </ul>
Network	1 dual-port network adapter, 1 Gbps or higher (2 network adapters can be used, but they need to be teamed with a single MAC address and a single IP address). Dual or multi-homed configurations are <b>not</b> supported for Video Interop Servers and Directors. Edge servers will require two network interfaces that are dual-port network adapters, 1 Gbps or higher (or two paired network adapters, for a total of four, each pair being teamed with a single MAC address and a single IP address, for a total of two pairs). On standalone Mediation Servers, the installation of additional network interface cards (NICs) to allow the configuration of a specific PSTN IP address is supported.

**NOTE**

Regardless of the server role, we also recommend the following hardware settings for Skype for Business Server 2019 (this may vary depending on the brand of hardware you've purchased, so please refer to manufacturer documentation for specifics):

- BIOS config - should be set to FLAT from NUMA.
- Enable Hyperthreading.
- The RSS queue setting should be set to 8 queue.

## Operating systems for Skype for Business Server 2019

After you have the hardware in place, you'll need to the install operating system (OS) that will allow you to install and successfully use Skype for Business Server 2019.

Windows Server 2019	
Windows Server 2016	

Anything other than the operating systems listed here won't work properly; please don't try it for installs of Skype for Business Server 2019. For example, Server Core option is not listed, and is thus not Supported.

## NOTE

If you are installing Windows Admin Center 2019 on your Windows Server 2019 machine, it will prompt you for a port to listen on. There's a likelihood you might choose port 443, but if that machine has Skype for Business Server 2019 installed on it, or is going to have Skype for Business Server 2019 installed on it, then you must choose a different port number.

Why is this the case? If Windows Admin Center 2019 is running on port 443, you will not be able to connect to the server using the Skype for Business Control Panel, nor will you be able to connect to any internal web service running on the server (Address Book Web Service, Autodiscover Service, WebTicket Service, etc). In fact, you will not be able to connect to any Internal Web Service URL. Please choose a different port, in the event you need or want to put Windows Admin Center 2019 on a server with Skype for Business Server 2019.

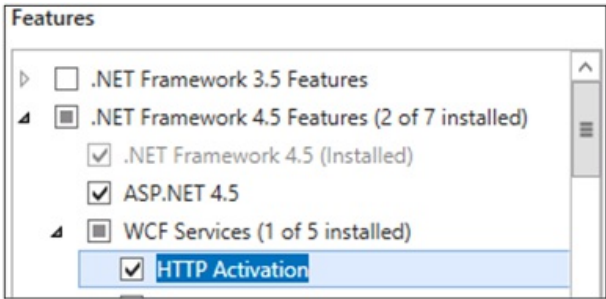
## Software that should be installed before a Skype for Business Server 2019 deployment

There are some things you're going to need to install or configure for any server running Skype for Business Server 2019. These are listed below, followed by additional requirements for specific server roles.

### IMPORTANT

Skype For Business 2019 supports .Net Framework 4.8.

### All servers:

SOFTWARE/ROLE	DETAILS
Windows PowerShell 3.0	All Skype for Business Server servers need Windows PowerShell 3.0 installed. <ul style="list-style-type: none"><li>• This should be installed by default with Windows Server 2016.</li></ul>
Microsoft .NET Framework	WCF services is a <b>Feature</b> that's installed as a Windows feature, under <b>Server Manager</b> , initially no downloads needed. <ul style="list-style-type: none"><li>• You need to make sure, when you install this feature, or if it's already installed and you're checking on it, that the <b>HTTP Activation</b> option is also checked and installed, like so:</li></ul>  <p>The screenshot shows the 'Features' window in Server Manager. It lists several features with checkboxes. Under '.NET Framework 4.5 Features (2 of 7 installed)', the following are checked: '.NET Framework 4.5 (Installed)', 'ASP.NET 4.5', and 'WCF Services (1 of 5 installed)'. Under 'WCF Services (1 of 5 installed)', 'HTTP Activation' is checked and highlighted in blue.</p> <ul style="list-style-type: none"><li>• Don't worry if you get an additional pop-up saying some other things need to be installed for HTTP Activation to be installed. That's normal; click OK and go ahead. If you don't get this pop-up, you can assume those things are already installed and go ahead.</li></ul> <p>Microsoft .NET Framework is usually installed when Windows Server 2016 is installed. Skype for Business Server requires Microsoft .NET Framework 4.7 or 4.8 though, so you'd probably need to update it. You can find the update <a href="#">here</a></p>

SOFTWARE/ROLE	DETAILS
Media Foundation	For Windows Server 2016, the Windows Media Format Runtime installs with Microsoft Media Foundation. All Front End Servers and Standard Edition servers used for conferencing require Windows Media Format Runtime to run the Windows Media Audio (.wma) files that the Call Park, Announcement, and Response Group applications play for announcements and music.
Windows Identity Foundation	We need Windows Identity Foundation 3.5 to support server-to-server authentication scenarios for Skype for Business Server 2019. • For Windows Server 2016, there's no need to download anything. Open <b>Server Manager</b> , and go to the <b>Add Roles and Features Wizard. Windows Identity Foundation 3.5</b> is listed under the <b>Features</b> section. If it's selected, you're good. Otherwise select it and click <b>Next</b> to reach the <b>Install</b> button.
Remote Server Administration Tools	Role Administration Tools: AD DS and AD LDS tools

**Front End Servers and Standard Edition server also need:**

SOFTWARE/ROLE	DETAILS
Internet Information Services (IIS)	IIS is needed on all Front End Servers, as well as all Standard Edition servers, with the following modules selected: <ul style="list-style-type: none"> <li>• Common HTTP Features: Default Document, HTTP Errors, Static Content</li> <li>• Health and Diagnostics: HTTP Logging, Logging Tools, Tracing</li> <li>• Performance: Static Content Compression, Dynamic Content Compression</li> <li>• Security: Request Filtering, Client Certificate Mapping Authentication, Windows Authentication</li> <li>• Application Development: .NET Extensibility 3.5, .NET Extensibility 4.5, ASP.NET 3.5, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters</li> <li>• Management Tools: IIS Management Console, IIS Management Scripts and Tools</li> </ul> Note that Anonymous Access is also needed, but you get that when you install IIS, so you don't have a place to select it on the list.
Windows Media Format Runtime	For Windows Server 2016, you'll need to install the <b>Media Foundation</b> feature in <b>Server Manager</b> . You actually can start your Skype for Business Server 2019 installation without this, but you'll be prompted to install it, and then reboot the server, before the Skype for Business Server 2019 install continues. It's better to do it ahead of time.
Silverlight	You can install the latest version of Silverlight <a href="#">here</a> .

To help you out, here's a sample PowerShell script you can run to automate this:

```
Add-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Asp-Net,
Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-
Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filtering, Web-Stat-Compression, Web-Dyn-
Compression, NET-WCF-HTTP-Activation45, Web-Asp-Net45, Web-Mgmt-Tools, Web-Scripting-Tools, Web-Mgmt-Compat,
Windows-Identity-Foundation, Server-Media-Foundation, Telnet-Client, BITS, ManagementOData, Web-Mgmt-Console,
Web-Metabase, Web-Lgcy-Mgmt-Console, Web-Lgcy-Scripting, Web-WMI, Web-Scripting-Tools, Web-Mgmt-Service
```

### **Directors also need:**

IIS, with the following modules selected:

- Common HTTP Features
  - Default Document
  - HTTP Errors
  - Static Content
- Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - Tracing
- Performance
  - Static Content Compression
- Security
  - Request Filtering
  - Client Certificate Mapping Authentication
  - Windows Authentication
- Application Development
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
  - ASP.NET 3.5
  - ASP.NET 4.5
  - ISAPI Extension
  - ISAPI Filters

(If you're wondering, it's the same module set as the Front End Servers and Standard Edition servers, with the Dynamic Content Compression and Management Tools left out.)

And we have some PowerShell code below for this too:

```
Add-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Asp-Net,
Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-
Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filtering, Web-Stat-Compression, NET-WCF-
HTTP-Activation45, Web-Asp-Net45, Web-Scripting-Tools, Web-Mgmt-Compat, Server-Media-Foundation, Telnet-Client
```

# Back end databases that will work with Skype for Business Server 2019

When installing Skype for Business Server 2019 Standard Edition, you'll have SQL Server 2016 Express (64-bit edition).

Skype for Business Server 2019 Enterprise Edition will require full SQL Server, as indicated below (only 64-bit edition; please don't use 32-bit editions):

Microsoft SQL Server 2019 (64-bit edition), and you must run with the latest updates.	Microsoft SQL Server 2017 (64-bit edition), and you must run with the latest updates.	
Microsoft SQL Server 2016 (64-bit edition), and you must run with the latest updates.		

If you don't see the SQL Server edition you want to use listed here, you can't use it.

## NOTE

You also need to install SQL Server Reporting Services for the Monitoring Server role.

## SQL Clustering, and SQL Always On

SQL Clustering with Skype for Business Server 2019 is supported. If you want to set up SQL Clustering, that's done in SQL Server.

Make sure you have an active/passive configuration for SQL Clustering, which is supported. Don't share the passive node with any other SQL instance.

You can have the following for failover clustering:

Two-node:

- Microsoft SQL Server 2019 Standard (64-bit edition), and we recommend running with the latest service pack.
- Microsoft SQL Server 2017 Standard (64-bit edition), and we recommend running with the latest service pack.
- Microsoft SQL Server 2016 Standard (64-bit edition), and we recommend running with the latest service pack.

Sixteen-node:

- Microsoft SQL Server 2019 Enterprise (64-bit edition), and we recommend running with the latest service pack.
- Microsoft SQL Server 2017 Enterprise (64-bit edition), and we recommend running with the latest service pack.
- Microsoft SQL Server 2016 Enterprise (64-bit edition), and we recommend running with the latest service pack.

SQL Always On is supported, and you can read more about it in [Back End Server high availability in Skype for Business Server 2019](#).

## Additional server installation recommendations:

Please don't install any Microsoft Internet Security and Acceleration (ISA) Server client software, or any other Winsock Layered Service Providers (LSP) software (any third-party firewalls or anti-virus network inspection software would be included here) on any of your front end servers or standalone mediation servers. Poor media

traffic performance has been seen when that software is installed.

## Active Directory

Although much of the configuration data for servers and services is stored in the Skype for Business Server 2019 Central Management store, there are some things still stored in Active Directory:

ACTIVE DIRECTORY OBJECTS	OBJECT TYPES
Schema extensions	User object extensions
	Extensions for Skype for Business Server 2015 and Lync Server 2013, to maintain backward compatibility with the previous supported versions
Data	User SIP URI and other user settings
	Contact objects for applications (like the Response Group application and the Conferencing Attendant application)
	Data published for backward compatibility
	A service control point (SCP) for the Central Management store
	Kerberos Authentication Account (an optional computer object)

### OS for Domain Controllers

The following Domain Controller operating systems can be used:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

The domain functional level of any domain you deploy Skype for Business Server 2019 into, and the forest functional level of any forest you deploy Skype for Business Server 2019 into, must be one of the following:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Can you have read-only domain controllers in these environments? Sure, as long as there are also writable domain controllers available.

It's important to know that Skype for Business Server 2019 doesn't support single-labeled domains. What are they? If you have a root domain labeled contoso.local, that's going to be fine. If you have a root domain that's just named local, that's not going to work, and it's not supported as a result. A little more about this has been written [in this Knowledge Base article](#).

Skype for Business Server 2019 also doesn't support renaming domains. If you really have to rename your domain, you'll need to uninstall Skype for Business Server 2019, do the domain rename, and then reinstall Skype for Business Server 2019.

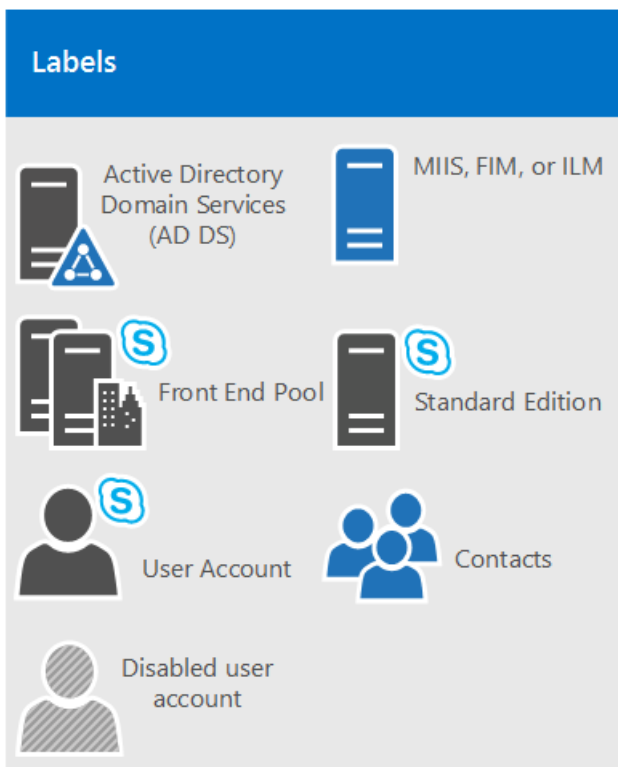
Finally, you may be dealing with a domain with a locked-down AD DS environment, and that's alright. We have more information on how to deploy Skype for Business Server 2019 into a locked-down AD DS environment in the Deployment documentation.

## AD Topologies

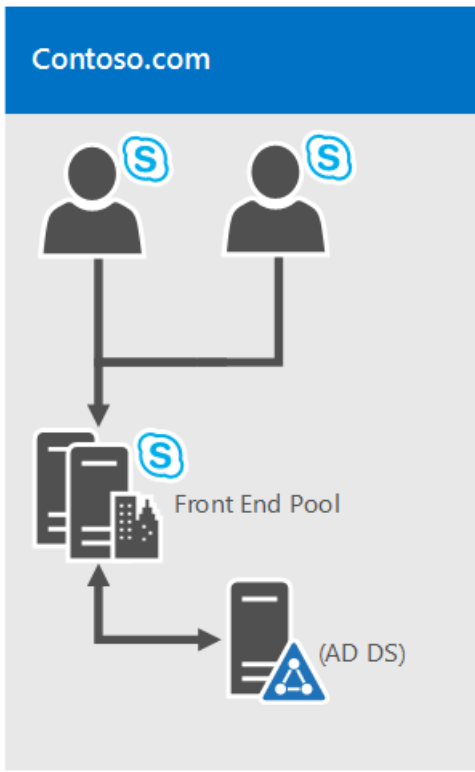
Supported topologies in Skype for Business Server 2019 are:

- Single forest with single domain
- Single forest with a single tree and multiple domains
- Single forest with multiple trees and disjoint namespaces
- Multiple forests in a central forest topology
- Multiple forests in a resource forest topology
- Multiple forests in a Skype for Business resource forest topology with Exchange Online
- Multiple forests in a resource forest topology with Skype for Business Online and Azure Active Directory Connect

We have diagrams and descriptions to help you determine what topology you have in your environment, or what you may need to set up prior to installing Skype for Business Server 2019. To keep it simple, we're also including a key:



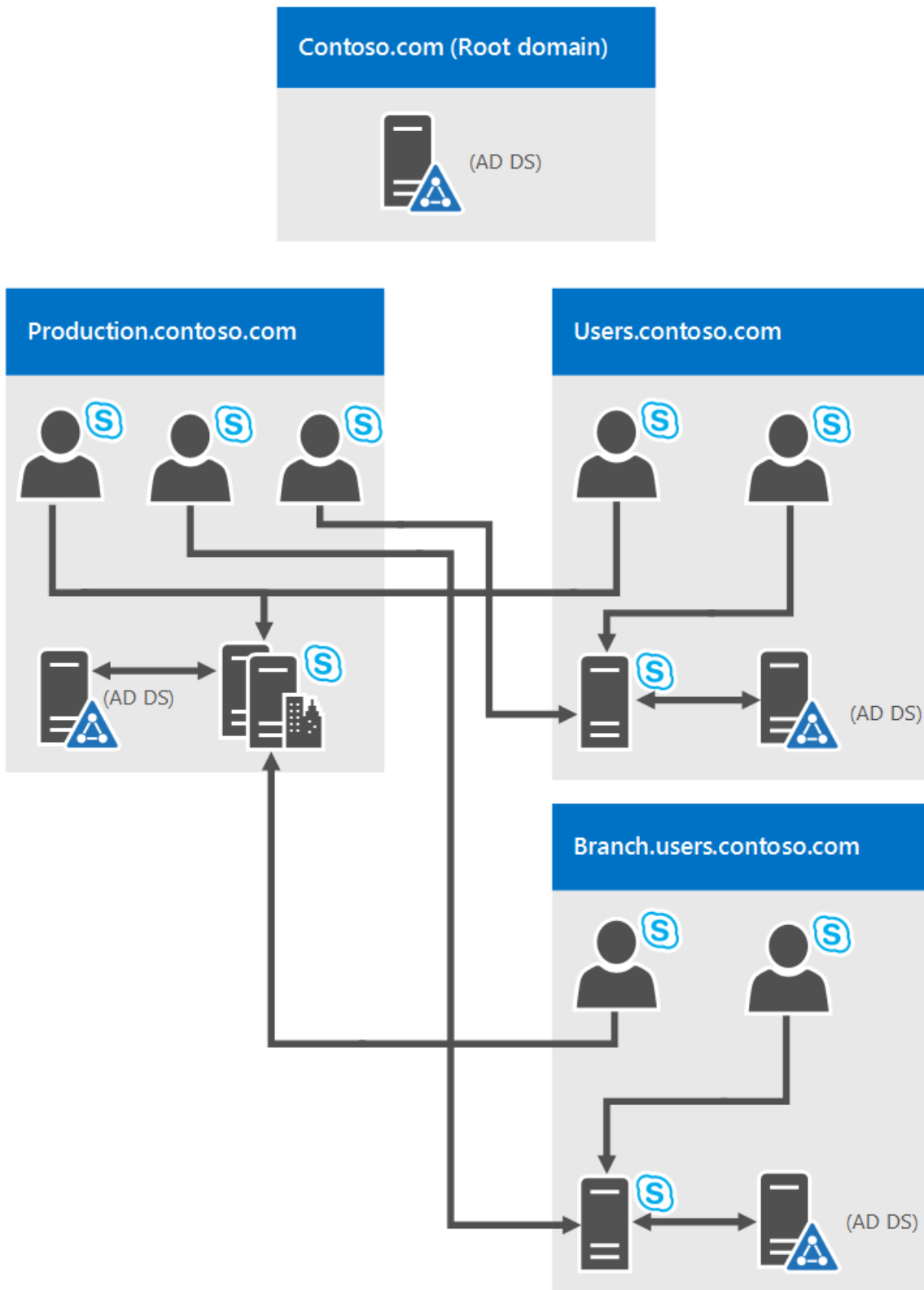
**Single forest with single domain**



It doesn't get easier than this; it's a single domain forest, a common topology.

**Single forest with a single tree and multiple domains**

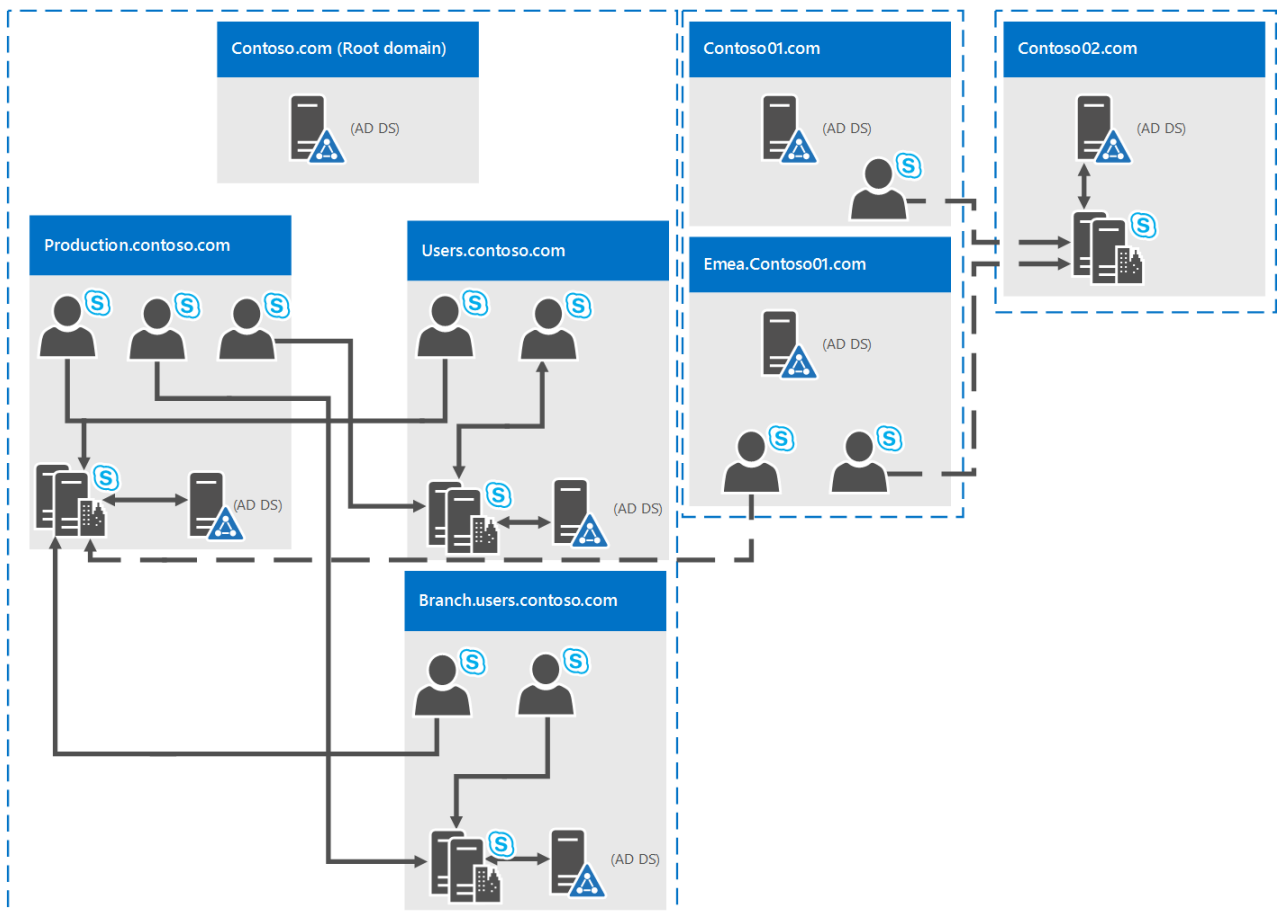




This diagram shows a single forest, again, but it has one or more child domains as well (there are three in this specific example). So the domain the users are created in might be different from the domain Skype for Business Server 2019 is deployed to. Why worry about this? It's important to remember that when you deploy a Skype for Business Server Front End pool, all the servers in that pool need to be in a single domain. You can have cross-domain administration via Skype for Business Server support of Windows universal administrator groups.

In the diagram above, you can see that users from one domain are able to access Skype for Business Server pools from the same domain or from different domains, even if those users are in a child domain.

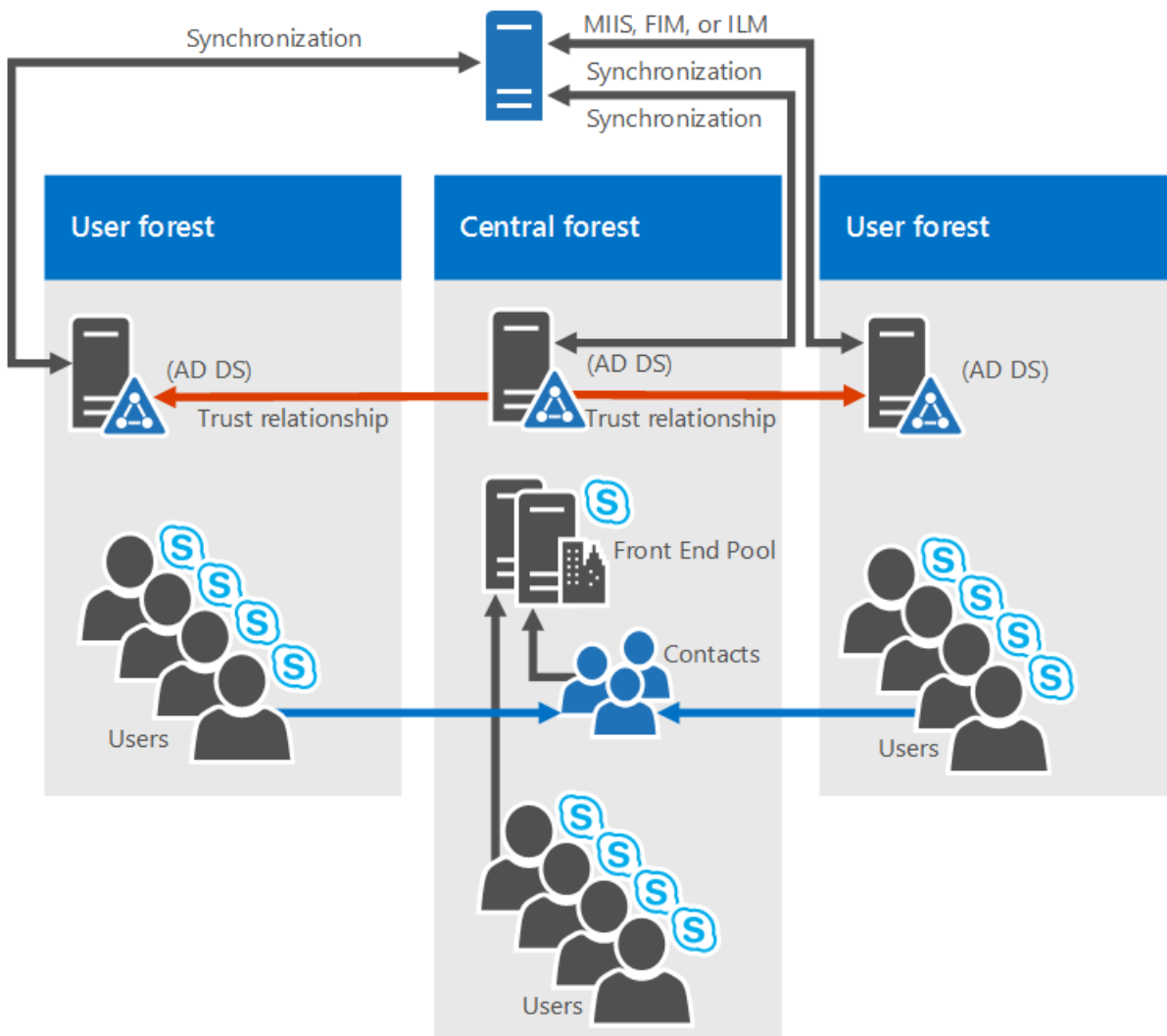
**Single forest with multiple trees and disjoint namespaces**



You may have a topology similar to this diagram, where you have one forest, but within that forest are multiple domains, with separate AD namespaces. In this case, this diagram is a good illustration, because it includes users in three different domains accessing Skype for Business Server 2019. Solid lines indicate they're accessing a Skype for Business Server pool in their own domain, whereas a dashed line indicates they're going to a pool in a different tree altogether.

As you can see, users in the same domain, the same tree, or even a different tree can access pools successfully.

#### **Multiple forests in a central forest topology**

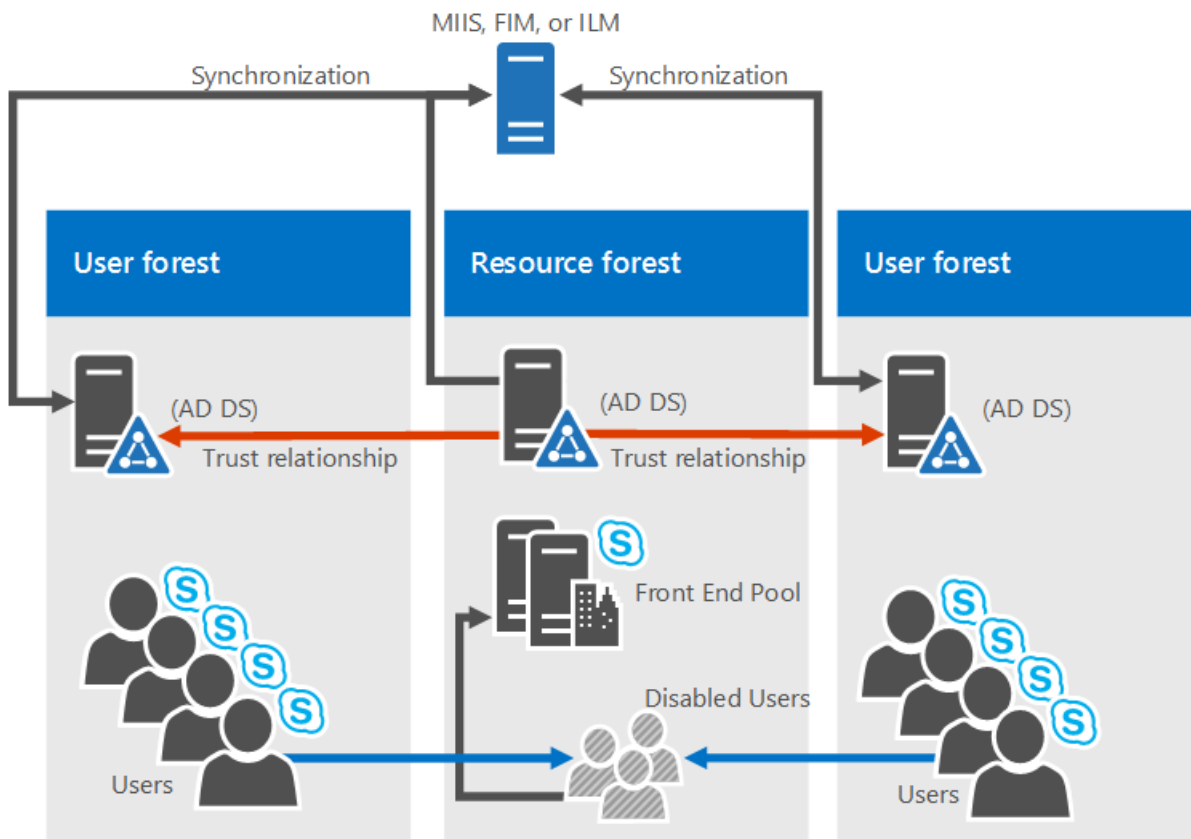


Skype for Business Server 2019 does support multiple forests configured in a central forest topology. If you're not sure that's what you have, the central forest in the topology uses objects in it to represent users in the other forests, and hosts user accounts for any users in the forest.

How does this work? A directory synchronization product (such as Forefront Identity Manager, or FIM) manages your organization's user accounts throughout their existence. When an account is created or deleted from a forest, that change is synched up to the corresponding contact in the central forest.

Clearly, if your AD infrastructure is in place, moving to this topology might not be easy, but if you're already there, or still planning out your forest infrastructure, this can be a good choice. You can centralize your Skype for Business Server 2019 deployment within a single forest, while users can search, communicate, and view the presence of other users in any forest. All user contact updates are handled automatically with synchronization software.

**Multiple forests in a Skype for Business resource forest topology**



A resource forest topology is also supported; it's where a forest is dedicated to running your server applications, like Microsoft Exchange Server and Skype for Business Server 2019. This resource forests also hosts a synchronized representation of active user objects, but no logon-enabled user accounts. So the resource forest is a shared services environment for other forests in which user objects reside, and they have a forest-level trust relationship with the resource forest.

Note that Exchange Server can be deployed in the same resource forest as Skype for Business Server or in a different forest.

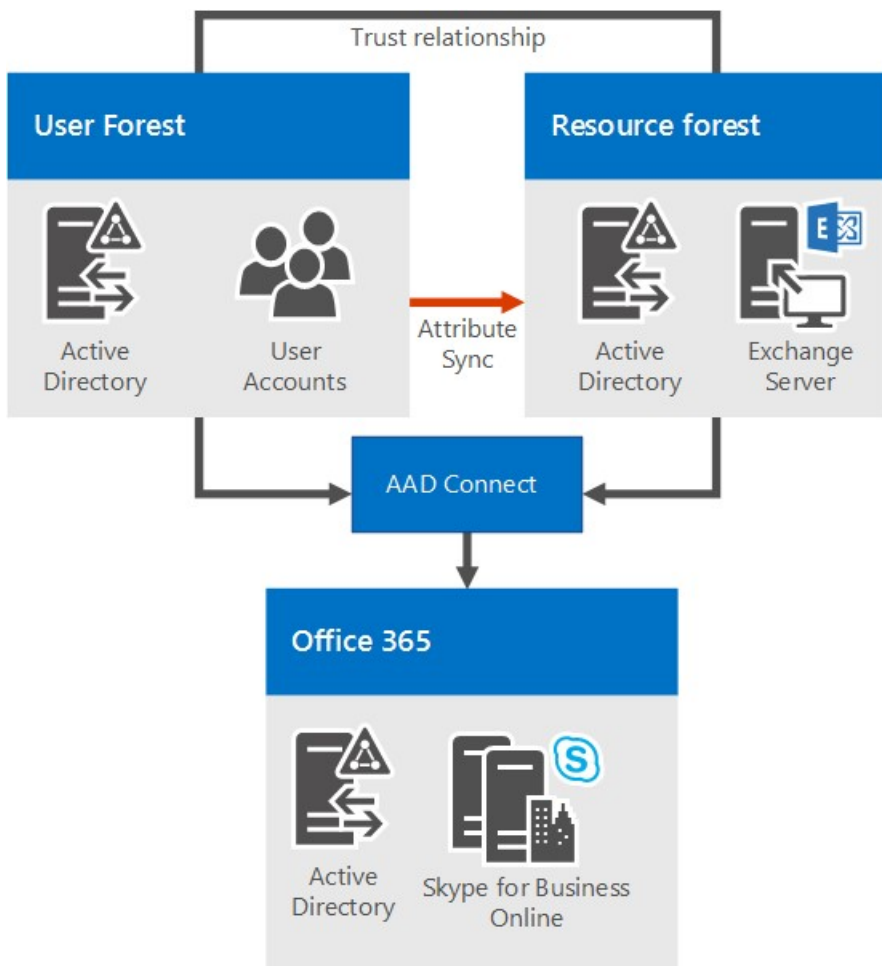
To deploy Skype for Business Server 2019 in this type of topology, you would create one disabled user object in the resource forest for each user account in the user forests (if Microsoft Exchange Server is already in the environment, this might be done for you). Then you need a directory synchronization tool (like Forefront Identity Manager, or FIM) to manage user accounts through their life cycle.

#### **Multiple forests in a Skype for Business resource forest topology with Exchange Online**

This topology is similar to the topology described in [Multiple forests in a Skype for Business resource forest topology](#).

In this topology, there are one or more user forests, and Skype for Business Server is deployed in a dedicated resource forest. Exchange Server can be deployed on-premises in the same resource forest or a different forest and configured for hybrid with Exchange Online, or email services may be provided exclusively by Exchange Online for the on-premises accounts. There is no diagram available for this topology.

#### **Multiple forests in a resource forest topology with Skype for Business Online and Azure Active Directory Connect**



With this scenario, there are multiple forests on-premises, with a resource forest topology. There is a full trust relationship between the Active Directory forests. The Azure Active Directory Connect tool is used to synchronize accounts between the on-premises user forests and Office 365.

The organization also has Office 365, and uses [Azure Active Directory Connect](#) to synchronize their on-premises accounts with Office 365. Users who are enabled for Skype for Business are enabled via Office 365 and Skype for Business Online. Skype for Business Server is not deployed on-premises.

Single sign-on authentication is provided by an Active Directory Federation Services farm located in the user forest.

In this scenario, it is supported to deploy Exchange on-premises, Exchange Online, a hybrid Exchange solution, or to not have Exchange deployed at all. (The diagram shows only Exchange on-premises, but the other Exchange solutions are also fully supported.)

#### **Multiple forests in a resource forest topology with hybrid Skype for Business**

In this scenario, there are one or more on-premises user forests, and Skype for Business is deployed in a dedicated resource forest and is configured for hybrid mode with Skype for Business Online. Exchange Server can be deployed on-premises in the same resource forest or a different forest and may be configured for hybrid with Exchange Online. Alternatively, email services may be provided exclusively by Exchange Online for the on-premises accounts.

For more information, see [Configure a multi-forest environment for hybrid Skype for Business](#).

## Domain Name System (DNS)

Skype for Business Server 2019 requires DNS, for the following reasons:

- DNS enables Skype for Business Server 2019 to discover internal servers or pools, allowing for server-to-server communications.

- DNS allows client machines to discover the Front End pool or Standard Edition server being used for SIP transactions.
- It associates simple URLs for conferences with the servers hosting those conferences.
- DNS allows external users and client machines to connect to your Edge Servers, or the HTTP reverse proxy, for instant messaging (IM) or conferencing.
- It lets unified communications (UC) devices that aren't logged in discover the Front End pool or Standard Edition server that's running the Device Update web service to get updates and send logs.
- Using DNS allows mobile clients to automatically discover web services resources without requiring users to manually enter URLs in their device settings.
- It's used in DNS load balancing.

It's important to note that Skype for Business Server 2019 doesn't support internationalized domain names (IDNs).

And it's extremely important to remember that any name in DNS be identical to the computer name configured on any server being used by Skype for Business Server 2019. Specifically, we can't have any short-names in the environment, and must have FQDNs for Topology Builder.

This seems like it would be logical for any computer already joined to a domain, but if you have an Edge Server that's not joined to your domain, it may have a default of a short name, with no domain suffix. Make sure that's not the case, either in DNS or on the Edge Server, or any Skype for Business Server 2019 server or pool, for that matter.

Definitely don't use Unicode characters or underscores. Standard characters (which are A-Z, a-z, 0-9, and hyphens) are supported by external DNS and public Certificate Authorities (you'll need to assign FQDNs to the SN in the certificate, it's important to remember), so you'll spare yourself a lot of trouble if you name with this in mind from the start.

For further reading on DNS requirements for Networking, check out the [Networking](#) section of our Planning documentation.

## Certificates

One of the most important things you can do before deploying is make sure you have your certificates in order. Skype for Business Server 2019 needs a public key infrastructure (PKI) for transport layer security (TLS) and mutual transport layer security (MTLS) connections. Basically, to communicate securely in a standardized way, Skype for Business Server uses certificates issued by Certificate Authorities (CAs).

These are some of the things that Skype for Business Server 2019 uses certificates for:

- TLS connections between clients and servers
- MTLS connections between servers
- Federation using automatic DNS discovery of partners
- Remote user access for instant messaging (IM)
- External user access to audio/video (AV) sessions, application sharing, and conferencing
- Talking to web applications and Outlook Web Access (OWA)

So certificate planning is a must. Now, let's look at a list of some of the things you need to keep in mind when requesting certificates:

- All server certificates must support server authorization (Server EKU).
- All server certificates must contain a CRL Distribution Point (CDP).
- All certificates must be signed using a signing algorithm supported by the operating system. Skype for Business Server 2019 supports the SHA-1 and SHA-2 suite of digest sizes (224, 256, 384 and 512-bit), and meets or exceeds the operating system requirements.
- Auto-enrollment is supported for internal servers running Skype for Business Server 2019.
- Auto-enrollment is not supported for Skype for Business Server 2019 Edge Servers.

#### NOTE

Using the RSASSA-PSS signature algorithm is unsupported, and may lead to errors on login and call forwarding issues, among other problems.

- Encryption key lengths of 1024, 2048, and 4096 are supported. Key lengths of 2048 and greater are recommended.
- The default digest, or hash signing, algorithm is RSA. The ECDH\_P256, ECDH\_P384, and ECDH\_P521 algorithms are also supported.

That's a lot to think about, and there are a variety of comfort levels with requesting certificates from a CA. We'll give you some further guidance below to make your planning as painless as possible.

#### Certificates for your internal servers

You'll need certificates for most of your internal servers, and most likely, you'll get them from an internal CA (that's a CA located in your domain). If you want to, you can request these certificates from an external CA (one located on the Internet). If you're wondering what public CA you should go to, you can check out the [Unified Communications certificate partners](#) list.

You're also going to need certificates when Skype for Business Server 2019 communicates with other applications and servers, such as Microsoft Exchange Server. This will, obviously, need to be a certificate that these other apps and servers can use in a supported way. Skype for Business Server 2019 and other Microsoft products support the Open Authorization (OAuth) protocol for server-to-server authentication and authorization. If you're interested in this, we have an additional planning article for OAuth and Skype for Business Server 2019.

Skype for Business Server 2019 also includes support for (without requiring) certificates signed using the SHA-256 cryptographic hash function. To support external access using SHA-256, the external certificate needs to be issued by a public CA using SHA-256.

To keep things straightforward, we've put the certificate requirements for Standard Edition servers, Front End pools, and other roles, into the following tables, with the fictional contoso.com being used for examples (you'll probably be using something else for your environment). These are all standard web server certificates, with private keys that are non-exportable. Some additional things to note:

- Server enhanced key usage (EKU) is automatically configured when you use the certificate wizard to request certificates.
- Each certificate friendly name has to be unique in the computer store.
- As per the sample names below, if you've configured sipinternal.contoso.com or sipexternal.contoso.com in your DNS, they need to be added to the certificate's Subject Alternative Name (SAN).

Certificates for Standard Edition servers:

CERTIFICATE	SUBJECT NAME/COMMON NAME	SUBJECT ALTERNATIVE NAME	EXAMPLE	COMMENTS
Default	FQDN of the pool	FQDN of the pool and FQDN of the server If you have multiple SIP domains and have enabled automatic client configuration, the certificate wizard detects and adds each supported SIP domain FQDNs. If this pool is the auto-logon server for clients and strict Domain Name System (DNS) matching is required in group policy, you also need entries for sip.sipdomain (for each SIP domain you have).	SN=se01.contoso.com; SAN=se01.contoso.com If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need SAN=sip.contoso.com; SAN=sip.fabrikam.com	On Standard Edition servers, the server FQDN is the same as the pool FQDN. The wizard detects any SIP domains you specified during setup and automatically adds them to the subject alternative name. You can also use this certificate for Server-to-Server Authentication.
Web internal	FQDN of the server	Each of the following: • Internal web FQDN (which is the same as the FQDN of the server) AND • Meet simple URLs • Dial-in simple URL • Admin simple URL OR • A wildcard entry for the simple URLs	SN=se01.contoso.com; SAN=se01.contoso.com; SAN=meet.contoso.com; SAN=meet.fabrikam.com; SAN=dialin.contoso.com; SAN=admin.contoso.com Using a wildcard certificate: SN=se01.contoso.com; SAN=se01.contoso.com; SAN=*.contoso.com	You can't override the Internal web FQDN in Topology Builder. If you have multiple Meet simple URLs, you must include all of them as SANs. Wildcard entries are supported for the simple URL entries.
Web external	FQDN of the server	Each of the following: • External web FQDN AND • Dial-in simple URL • Meet simple URLs per SIP domain OR • A wildcard entry for the simple URLs	SN=se01.contoso.com; SAN=webcon01.contoso.com; SAN=meet.contoso.com; SAN=meet.fabrikam.com; SAN=dialin.contoso.com Using a wildcard certificate: SN=se01.contoso.com; SAN=webcon01.contoso.com; SAN=*.contoso.com	If you have multiple Meet simple URLs, you must include all of them as subject alternative names. Wildcard entries are supported for the simple URL entries.



Certificates for Front End Servers in a Front End pool:

CERTIFICATE	SUBJECT NAME/Common Name	SUBJECT ALTERNATIVE NAME	EXAMPLE	COMMENTS
Default	FQDN of the pool	<p>FQDN of the pool and FQDN of the server</p> <p>If you have multiple SIP domains and have enabled automatic client configuration, the certificate wizard detects and adds each supported SIP domain FQDNs.</p> <p>If this pool is the auto-logon server for clients and strict Domain Name System (DNS) matching is required in group policy, you also need entries for sip.sipdomain (for each SIP domain you have).</p>	<p>SN=eepool.contoso.com;            SAN=eepool.contoso.com;            SAN=ee01.contoso.com</p> <p>If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need</p> <p>SAN=sip.contoso.com;            SAN=sip.fabrikam.com</p>	<p>The wizard detects any SIP domains you specified during setup and automatically adds them to the subject alternative name.</p> <p>You can also use this certificate for Server-to-Server Authentication.</p>
Web internal	FQDN of the pool	<p>Each of the following:</p> <ul style="list-style-type: none"> <li>• Internal web FQDN (which is NOT the same as the FQDN of the server)</li> <li>• Server FQDN</li> <li>• Skype for Business pool FQDN</li> </ul> <p>AND</p> <ul style="list-style-type: none"> <li>• Meet simple URLs</li> <li>• Dial-in simple URL</li> <li>• Admin simple URL</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• A wildcard entry for the simple URLs</li> </ul>	<p>SN=ee01.contoso.com;            SAN=ee01.contoso.com;            SAN=meet.contoso.com;            SAN=meet.fabrikam.com;            SAN=dialin.contoso.com;            SAN=admin.contoso.com</p> <p>Using a wildcard certificate:            SN=ee01.contoso.com;            SAN=ee01.contoso.com;            SAN=*.contoso.com</p>	<p>If you have multiple Meet simple URLs, you must include all of them as subject alternative names. Wildcard entries are supported for the simple URL entries.</p>

CERTIFICATE	SUBJECT NAME/COMMON NAME	SUBJECT ALTERNATIVE NAME	EXAMPLE	COMMENTS
Web external	FQDN of the pool	Each of the following: <ul style="list-style-type: none"> <li>• External web FQDN</li> </ul> AND <ul style="list-style-type: none"> <li>• Dial-in simple URL</li> <li>• Admin simple URL</li> </ul> OR <ul style="list-style-type: none"> <li>• A wildcard entry for the simple URLs</li> </ul>	SN=ee01.contoso.com; SAN=webcon01.contoso.com; SAN=meet.contoso.com; SAN=meet.fabrikam.com; SAN=dialin.contoso.com Using a wildcard certificate: SN=ee01.contoso.com; SAN=webcon01.contoso.com; SAN=*.contoso.com	If you have multiple Meet simple URLs, you must include all of them as subject alternative names. Wildcard entries are supported for the simple URL entries.

Certificates for the Director:

CERTIFICATE	SUBJECT NAME/COMMON NAME	SUBJECT ALTERNATIVE NAME	EXAMPLE
Default	Director pool	FQDN of the Director, FQDN of the Director pool. If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you'll also need entries for sip.sipdomain (for each SIP domain you have).	pool.contoso.com; SAN=dir01.contoso.com If this Director pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need SAN=sip.contoso.com; SAN=sip.fabrikam.com
Web internal	FQDN of the server	Each of the following: <ul style="list-style-type: none"> <li>• Internal web FQDN (which is the same as the FQDN of the server)</li> <li>• Server FQDN</li> <li>• Skype for Business pool FQDN</li> </ul> AND <ul style="list-style-type: none"> <li>• Meet simple URLs</li> <li>• Dial-in simple URL</li> <li>• Admin simple URL</li> </ul> OR <ul style="list-style-type: none"> <li>• A wildcard entry for the simple URLs</li> </ul>	SN=dir01.contoso.com; SAN=dir01.contoso.com; SAN=meet.contoso.com; SAN=meet.fabrikam.com; SAN=dialin.contoso.com; SAN=admin.contoso.com Using a wildcard certificate: SN=dir01.contoso.com; SAN=dir01.contoso.com SAN=*.contoso.com

CERTIFICATE	SUBJECT NAME/COMMON NAME	SUBJECT ALTERNATIVE NAME	EXAMPLE
Web external	FQDN of the server	Each of the following: <ul style="list-style-type: none"> <li>External web FQDN</li> </ul> AND <ul style="list-style-type: none"> <li>Meet simple URLs per SIP domain</li> <li>Dial-in simple URL</li> </ul> OR <ul style="list-style-type: none"> <li>A wildcard entry for the simple URLs</li> </ul>	The Director external web FQDN must be different from the Front End pool or Front End Server. SN=dir01.contoso.com; SAN=directorwebcon01.contoso.com SAN=meet.contoso.com; SAN=meet.fabrikam.com; SAN=dialin.contoso.com Using a wildcard certificate: SN=dir01.contoso.com; SAN=directorwebcon01.contoso.com SAN=*.contoso.com

Certificates for Stand-alone Mediation Server:

CERTIFICATE	SUBJECT NAME/COMMON NAME	SUBJECT ALTERNATIVE NAME	EXAMPLE
Default	FQDN of the pool	FQDN of the pool FQDN of the pool member server	SN=medsvr-pool.contoso.net; SAN=medsvr-pool.contoso.net; SAN=medsvr01.contoso.net

Certificates for Survivable Branch Appliance (Specifically, Survivable Branch Appliance 2015 for Skype for Business Server 2019):

CERTIFICATE	SUBJECT NAME/COMMON NAME	SUBJECT ALTERNATIVE NAME	EXAMPLE
Default	FQDN of the appliance	SIP.<sipdomain> (you need only one entry per SIP domain)	SN=sba01.contoso.net; SAN=sip.contoso.com; SAN=sip.fabrikam.com

**Certificates for external user access (Edge)**

Skype for Business Server 2019 supports the use of a **single public certificate** for access and web conferencing Edge external interfaces, plus the A/V Authentication service, which is all provided via the Edge Server(s). Your Edge internal interface will typically use a private certificate issued by your internal CA, but if you'd prefer, you can use a public certificate for this as well, if it's from a trusted CA.

Your reverse proxy (RP) is also going to use a public certificate, and it encrypts the communication from your RP to clients, and the RP to internal servers by using HTTP (or more precisely, TLS over HTTP).

**Certificates for mobility**

If you're deploying mobility and you're supporting automatic discovery for mobile clients, you're going to need to include some additional subject alternate name entries on your certificates to support the secure connections from the mobile clients.

You'll need SAN names for automatic discovery on the following certificates:

- Director pool
- Front End pool

- Reverse Proxy

The specifics are listed in the tables below.

This is where a little pre-planning is good, but sometimes you've deployed Skype for Business Server 2019 without intending to deploy mobility, and that comes up later when you already have certificates in your environment. Reissuing them via an internal CA is typically pretty easy, but with public certificates from a public CA, that can be a little more pricy.

If that's what you're looking at, and if you have a lot of SIP domains (which would make adding SANS more expensive), you can configure your reverse proxy to use HTTP for the initial Autodiscover Service request, instead of using HTTPS (which is the default configuration). The [Plan for Mobility](#) article has more information on this.

Director pool and Front End pool certificate requirements:

DESCRIPTION	SAN ENTRY
Internal Autodiscover service URL	SAN=lyncdiscoverinternal.<sipdomain>
External Autodiscover service URL	SAN=lyncdiscover.<sipdomain>

You can alternatively use SAN=\*.<sipdomain>

Reverse Proxy (Public CA) certificate requirements:

DESCRIPTION	SAN ENTRY
External Autodiscover service URL	SAN=lyncdiscover.<sipdomain>

This SAN needs to be assigned to the certificate that's assigned to the SSL Listener on your reverse proxy.

#### NOTE

Your reverse proxy listener is going to have SANs for your external Web Services URL(s). Some examples would be SAN=skypewebextpool01.contoso.com and dirwebexternal.contoso.com, if you've deployed the Director, (which is optional).

## File Share

Skype for Business Server 2019 can use the same file share for all file storage. You do need to keep the following in mind:

- A file share needs to be on either direct attached storage (DAS) or a storage area network (SAN), and this includes the Distributed File System (DFS) as well as a redundant array of independent disks (RAID) for file stores. For further reading on DFS for Windows Server 2012, check out [this DFS page](#).
- We recommend a shared cluster for the file share. If you're already using one, you should cluster Windows Server 2012 or higher versions

#### NOTE

**Why the latest Windows?** Older versions may not have the right permissions to enable all features. You can use Cluster Administrator to create the file shares. See this support article [How to create file shares on a cluster](#) for more details.

#### Caution

You should know that using network attached storage (NAS) as a file share isn't supported, so use one of the

options listed above. This support limitation is caused by the variable design of NAS devices that have to provide file system adaptability to the Windows Server-based computer that accesses the devices' shared file system.

# Load balancing requirements for Skype for Business

5/20/2019 • 17 minutes to read

**Summary:** Review the load balancing considerations before implementing Skype for Business Server.

Load balancing distributes traffic among the servers in a pool. If you have Front End pools, Mediation Server pools, or Edge Server pools, you need to deploy load balancing for these pools.

Skype for Business Server supports two types of load balancing solutions for client-to-server traffic: Domain Name System (DNS) load balancing and hardware load balancing (often abbreviated as HLB). DNS load balancing offers several advantages including simpler administration, more efficient troubleshooting, and the ability to isolate much of your Skype for Business Server traffic from any potential hardware load balancer problems.

Decide for yourself which load balancing solution is appropriate for each pool in your deployment, but keep in mind the following restrictions:

- The internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one interface and hardware load balancing on the other.
- Some types of traffic require a hardware load balancer. For example, HTTP traffic requires a hardware load balancer instead of DNS load balancing. DNS load balancing does not work with client-to-server web traffic.

If you choose to use DNS load balancing for a pool but still need to implement hardware load balancers for traffic such as HTTP traffic, the administration of the hardware load balancers is greatly simplified. For example, configuring the hardware load balancer will be simpler as it will only manage the HTTP and HTTPS traffic, while all other protocols will be managed by DNS load balancing. For details, see [DNS Load Balancing](#).

For server-to-server traffic, Skype for Business Server uses topology-aware load balancing. Servers read the published topology in the Central Management store to obtain the FQDNs of servers in the topology, and automatically distribute the traffic among the servers. Administrators do not need to set up or manage this type of load balancing.

If you use DNS load balancing and you need to block traffic to a specific computer, it is not sufficient to just remove the IP address entries from the Pool FQDN. You must remove the DNS entry for the computer as well.

## Hardware load balancer requirements

The Skype for Business Server scaled consolidated Edge topology is optimized for DNS load balancing for new deployments federating primarily with other organizations using Skype for Business Server or Lync Server. If high availability is required for any of the following scenarios, a hardware load balancer must be used on Edge Server pools for the following:

- Federation with organizations using Office Communications Server 2007 R2 or Office Communications Server 2007
- Exchange UM for remote users using Exchange UM prior to Exchange 2010 with SP1
- Connectivity to public IM users

## IMPORTANT

Using DNS load balancing on one interface and hardware load balancing on the other is not supported. You must use hardware load balancing for both interfaces or DNS load balancing for both.

## NOTE

If you are using a hardware load balancer, the load balancer deployed for connections with the internal network must be configured to load balance only the traffic to servers running the Access Edge service and the A/V Edge service. It cannot load balance the traffic to the internal Web Conferencing Edge service or the internal XMPP Proxy service.

## NOTE

The direct server return (DSR) NAT is not supported with Skype for Business Server.

To determine whether your hardware load balancer supports the necessary features required by Skype for Business Server, see [Infrastructure for Skype for Business](#).

### Hardware Load Balancer Requirements for Edge Servers Running the A/V Edge Service

Following are the hardware load balancer requirements for Edge Servers running the A/V Edge service:

- Turn off TCP nagling for both internal and external ports 443. Nagling is the process of combining several small packets into a single, larger packet for more efficient transmission.
- Turn off TCP nagling for external port range 50,000 - 59,999.
- Do not use NAT on the internal or external firewall.
- The edge internal interface must be on a different network than the Edge Server external interface and routing between them must be disabled.
- The external interface of the Edge Server running the A/V Edge Service must use publicly routable IP addresses and no NAT or port translation on any of the edge external IP addresses.
- The load balancer must not change the source address of the client.

### Other Hardware Load Balancer requirements

Cookie-based affinity requirements are greatly reduced in Skype for Business Server for Web services. If you are deploying Skype for Business Server and will not retain any Lync Server 2010 Front End Servers or Front End pools, you do not need cookie-based persistence. However, if you will temporarily or permanently retain any Lync Server 2010 Front End Servers or Front End pools, you still use cookie-based persistence as it is deployed and configured for Lync Server 2010.

## NOTE

**If you decide to use cookie-based affinity even though your deployment does not require it**, there is no negative impact to doing so.

For deployments that **will not use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.

For deployments that **will use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.
- Hardware load balancer cookie MUST NOT be marked httpOnly
- Hardware load balancer cookie MUST NOT have an expiration time
- Hardware load balancer cookie MUST be named **MS-WSMAN** (This is the value that the Web services expect, and cannot be changed)
- Hardware load balancer cookie MUST be set in every HTTP response for which the incoming HTTP request did not have a cookie, regardless of whether a previous HTTP response on that same TCP connection had already obtained a cookie. If the load balancer optimizes cookie insert to only occur once per TCP connection, that optimization MUST NOT be used

**NOTE**

Typical hardware load balancer configurations use source-address affinity and a 20 min. TCP session lifetime, which is fine for Lync Server and Lync 2013 clients because session state is maintained through client usage and/or application interaction.

If you are deploying mobile devices, your hardware load balancer must be able to load balance individual request within a TCP session (in effect, you must be able to load balance an individual request based on the target IP address).

**Caution**

If you are deploying mobile devices, your hardware load balancer must be able to individually load balance each request within a TCP connection. The latest Apple iOS mobile apps require Transport Layer Security (TLS) version 1.2.

**Caution**

For details on third party hardware load balancers, see [Infrastructure for Skype for Business](#).

Following are the hardware load balancer requirements for Director and Front End pool Web Services:

- For internal Web Services VIPs, set Source\_addr persistence (internal port 80, 443) on the hardware load balancer. For Skype for Business Server, Source\_addr persistence means that multiple connections coming from a single IP address are always sent to one server to maintain session state.
- Use TCP idle timeout of 1800 seconds.
- On the firewall between the reverse proxy and the next hop pool's hardware load balancer, create a rule to allow https: traffic on port 4443, from the reverse proxy to the hardware load balancer. The hardware load balancer must be configured to listen on ports 80, 443, and 4443.

**Summary of Hardware Load Balancer Affinity Requirements**

CLIENT/USER LOCATION	EXTERNAL WEB SERVICES FQDN AFFINITY REQUIREMENTS	INTERNAL WEB SERVICES FQDN AFFINITY REQUIREMENTS
Lync Web App (internal and external users) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (external users only) Mobile device (internal and external users)	No affinity	Source address affinity



CLIENT/USER LOCATION	EXTERNAL WEB SERVICES FQDN AFFINITY REQUIREMENTS	INTERNAL WEB SERVICES FQDN AFFINITY REQUIREMENTS
Lync Web App (internal users only) Mobile device (not deployed)	No affinity	Source address affinity

### Port Monitoring for Hardware Load Balancers

You define port monitoring on the hardware load balancers to determine when specific services are no longer available due to hardware or communications failure. For example, if the Front End Server service (RTCSRVR) stops because the Front End Server or Front End pool fails, the HLB monitoring should also stop receiving traffic on the Web Services. You implement port monitoring on the HLB to monitor the following:

#### Front End Server User Pool - HLB Internal Interface

VIRTUAL IP/PORT	NODE PORT	NODE MACHINE/MONITOR	PERSISTENCE PROFILE	NOTES
<pool>web-int_mco_443_vs_443	443	Front End 5061	Source	HTTPS
<pool>web-int_mco_80_vs_80	80	Front End 5061	Source	HTTP

#### Front End Server User Pool - HLB External Interface

VIRTUAL IP/PORT	NODE PORT	NODE MACHINE/MONITOR	PERSISTENCE PROFILE	NOTES
<pool>web_mco_443_vs_443	4443	Front End 5061	None	HTTPS
<pool>web_mco_80_vs_80	8080	Front End 5061	None	HTTP

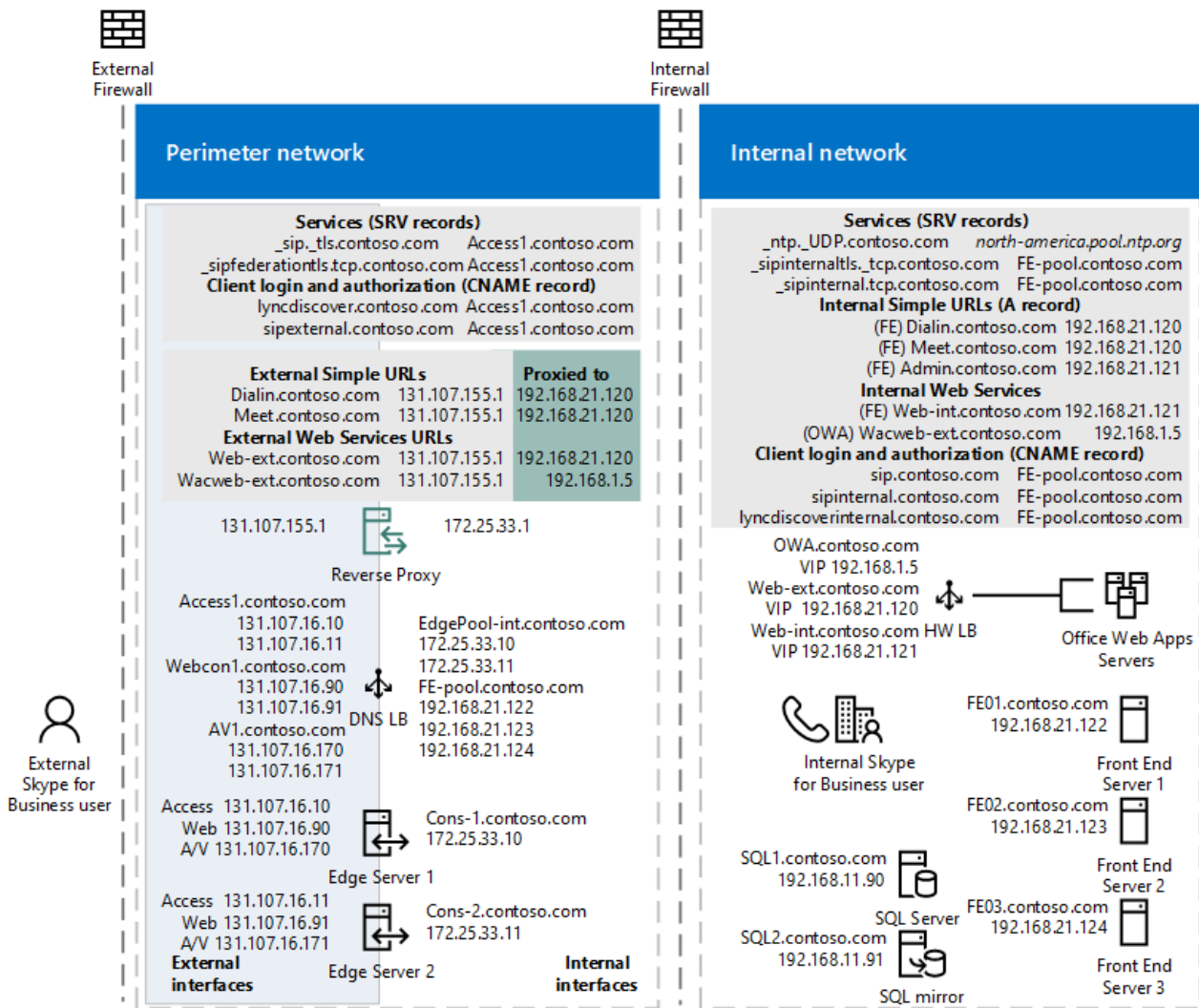
## DNS Load Balancing

Skype for Business Server enables DNS load balancing, a software solution that can greatly reduce the administration overhead for load balancing on your network. DNS load balancing balances the network traffic that is unique to Skype for Business Server, such as SIP traffic and media traffic.

If you deploy DNS load balancing, your organization's administration overhead for hardware load balancers will be minimized. Additionally, complex troubleshooting of problems related to misconfiguration of load balancers for SIP traffic will be eliminated. You can also prevent server connections so that you can take servers offline. DNS load balancing also ensures that hardware load balancer problems do not affect elements of SIP traffic such as basic call routing.

The following diagram shows an example that includes both internal and external DNS load balancing:

#### Edge network diagram using Public IPv4 addresses



If you use DNS load balancing, you may also be able to purchase lower-cost hardware load balancers than if you used the hardware load balancers for all types of traffic. You should use load balancers that have passed interoperability qualification testing with Skype for Business Server. For details about load balancer interoperability testing, see [Lync Server 2010 Load Balancer Partners](#). The content there applies to Skype for Business Server.

DNS load balancing is supported for Front End pools, Edge Server pools, Director pools, and stand-alone Mediation Server pools.

DNS load balancing is typically implemented at the application level. The application (for example, a client running Skype for Business), tries to connect to a server in a pool by connecting to one of the IP addresses returned from the DNS A and AAAA (if IPv6 addressing is used) record query for the pool fully qualified domain name (FQDN).

For example, if there are three front end servers in a pool named pool01.contoso.com, the following will happen:

- Clients running Skype for Business query DNS for pool01.contoso.com. The query returns three IP addresses and caches them as follows (not necessarily in this order):
  - pool01.contoso.com 192.168.10.90
  - pool01.contoso.com 192.168.10.91
  - pool01.contoso.com 192.168.10.92
- The client attempts to establish a Transmission Control Protocol (TCP) connection to one of the IP addresses. If that fails, the client tries the next IP address in the cache.
- If the TCP connection succeeds, the client negotiates TLS to connect to the primary registrar on pool01.contoso.com.

- If the client tries all cached entries without a successful connection, the user is notified that no servers running Skype for Business Server are available at the moment.

#### NOTE

DNS-based load balancing is different from DNS round robin (DNS RR) which typically refers to load balancing by relying on DNS to provide a different order of IP addresses corresponding to the servers in a pool. Typically DNS RR only enables load distribution, but does not enable failover. For example, if the connection to the one IP address returned by the DNS A and AAAA (if you are using IPv6 addressing) query fails, the connection fails. Therefore, DNS round robin by itself is less reliable than DNS-based load balancing. You can use DNS round robin in conjunction with DNS load balancing.

DNS load balancing is used for the following:

- Load balancing server-to-server SIP to the Edge Servers
- Load balancing Unified Communications Application Services (UCAS) applications such as Conferencing, Auto Attendant, Response Group, and Call Park
- Preventing new connections to UCAS applications (also known as "draining")
- Load balancing all client-to-server traffic between clients and Edge Servers

DNS load balancing cannot be used for the following:

- Client-to-server web traffic to Director or Front End Servers

DNS load balancing and federated traffic:

If multiple DNS records are returned by a DNS SRV query, the Access Edge service always picks the DNS SRV record with the lowest numeric priority and highest numeric weight. The Internet Engineering Task Force document "A DNS RR for specifying the location of services (DNS SRV)" [RFC 2782, DNS SRV RR](#) specifies that if there are multiple DNS SRV records defined, priority is first used, then weight. For example, DNS SRV record A has a weight of 20 and a priority of 40 and DNS SRV record B has a weight of 10 and priority of 50. DNS SRV record A with priority 40 will be selected. The following rules apply to DNS SRV record selection:

- Priority is considered first. A client MUST attempt to contact the target host defined by the DNS SRV record with the lowest numbered priority it can reach. Targets with the same priority SHOULD be tried in an order defined by the weight field.
- The weight field specifies a relative weight for entries with the same priority. Larger weights SHOULD be given a proportionately higher probability of being selected. DNS administrators SHOULD use Weight 0 when there isn't any server selection to do. In the presence of records containing weights greater than 0, records with weight 0 should have a very small chance of being selected.

If multiple DNS SRV records with equal priority and weight are returned, the Access Edge service will select the SRV record that was received first from the DNS server.

#### **DNS Load Balancing on Front End Pools and Director Pools**

You can use DNS load balancing for the SIP traffic on Front End pools and Director pools. With DNS load balancing deployed, you still need to also use hardware load balancers for these pools, but only for client-to-server HTTPS traffic. The hardware load balancer is used for HTTPS traffic from clients over ports 443 and 80.

Although you still need hardware load balancers for these pools, their setup and administration will be primarily for HTTPS traffic, which the administrators of hardware load balancers are accustomed to.

#### **DNS Load Balancing and Supporting Older Clients and Servers**

DNS load balancing supports automatic failover only for servers running Skype for Business Server or Lync Server 2010, and for Lync 2013 and Skype for Business clients. Earlier versions of clients and Office

Communications Server can still connect to pools running DNS load balancing, but if they cannot make a connection to the first server that DNS load balancing refers them to, they are unable to fail over to another server in the pool.

Additionally, if you are using Exchange UM, you must use a minimum of Exchange 2010 SP1 to get support for Skype for Business Server DNS load balancing. If you use an earlier version of Exchange, your users will not have failover capabilities for these Exchange UM scenarios:

- Playing their Enterprise voicemail on their phone
- Transferring calls from an Exchange UM Auto Attendant

All other Exchange UM scenarios will work properly.

#### Deploying DNS Load Balancing on Front End Pools and Director Pools

Deploying DNS load balancing on Front End pools and Director pools requires you to perform a couple of extra steps with FQDNs and DNS records.

- A pool that uses DNS load balancing must have two FQDNs: the regular pool FQDN that is used by DNS load balancing (such as pool01.contoso.com), and resolves to the physical IPs of the servers in the pool, and another FQDN for the pool's Web services (such as web01.contoso.com), which resolves to virtual IP address of the pool.

In Topology Builder, if you want to deploy DNS load balancing for a pool, to create this extra FQDN for the pool's Web services you must select the **Override internal Web Services pool FQDN** check box and type the FQDN, in the **Specify the Web Services URLs for this Pool** page.

- To support the FQDN used by DNS load balancing, you must provision DNS to resolve the pool FQDN (such as pool01.contoso.com) to the IP addresses of all the servers in the pool (for example, 192.168.1.1, 192.168.1.2, and so on). You should include only the IP addresses of servers that are currently deployed.

#### Caution

If you have more than one Front End pool or Front End Server the external Web services FQDN must be unique. For example, if you define the external Web services FQDN of a Front End Server as **pool01.contoso.com**, you cannot use **pool01.contoso.com** for another Front End pool or Front End Server. If you are also deploying Directors, the external Web services FQDN defined for any Director or Director pool must be unique from any other Director or Director pool as well as any Front End pool or Front End Server. If decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool.

#### DNS Load Balancing on Edge Server Pools

You can deploy DNS load balancing on Edge Server pools. If you do, you must be aware of some considerations.

Using DNS load balancing on your Edge Servers causes a loss of failover ability in the following scenarios:

- Federation with organizations that are running versions of Skype for Business Server released prior to Lync Server 2010.
- Instant message exchange with users of public instant messaging (IM) services AOL and Yahoo!, in addition to XMPP-based providers and servers, such as Google Talk, currently the only supported XMPP partner.

These scenarios will work as long as all Edge Servers in the pool are up and running, but if one Edge Server is unavailable, any requests for these scenarios that are sent to it will fail, instead of routing to another Edge Server.

If you are using Exchange UM, you must use a minimum of Exchange 2013 to get support for Skype for Business Server DNS load balancing on Edge. If you use an earlier version of Exchange, your remote users will not have failover capabilities for these Exchange UM scenarios:

- Playing their Enterprise voicemail on their phone

- Transferring calls from an Exchange UM Auto Attendant

All other Exchange UM scenarios will work properly.

The internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one Edge interface and hardware load balancing on the other Edge interface.

#### **Deploying DNS Load Balancing on Edge Server Pools**

To deploy DNS load balancing on the external interface of your Edge Server pool, you need the following DNS entries:

- For the Access Edge service, you need one entry for each server in the pool. Each entry must resolve the FQDN of the Access Edge service (for example, sip.contoso.com) to the IP address of the Access Edge service on one of the Edge Servers in the pool.
- For the Web Conferencing Edge service, you need one entry for each server in the pool. Each entry must resolve the FQDN of the Web Conferencing Edge service (for example, webconf.contoso.com) to the IP address of the Web Conferencing Edge service on one of the Edge Servers in the pool.
- For the Audio/Video Edge service, you need one entry for each server in the pool. Each entry must resolve the FQDN of the Audio/Video Edge service (for example, av.contoso.com) to the IP address of the A/V Edge service on one of the Edge Servers in the pool.

To deploy DNS load balancing on the internal interface of your Edge Server pool, you must add one DNS A record, which resolves the internal FQDN of the Edge Server pool to the IP address of each server in the pool.

#### **Using DNS Load Balancing on Mediation Server Pools**

You can use DNS load balancing on stand-alone Mediation Server pools. All SIP and media traffic is balanced by DNS load balancing.

To deploy DNS load balancing on a Mediation Server pool, you must provision DNS to resolve the pool FQDN (for example, mediationpool1.contoso.com) to the IP addresses of all the servers in the pool (for example, 192.168.1.1, 192.168.1.2, and so on).

#### **Blocking Traffic to a Server With DNS Load Balancing**

If you use DNS load balancing and you need to block traffic to a specific computer, it is not sufficient to just remove the IP address entries from the Pool FQDN. You must remove the DNS entry for the computer as well.

Note that for server-to-server traffic, Skype for Business Server uses topology-aware load balancing. Servers read the published topology in the Central Management store to obtain the FQDNs of servers in the topology, and automatically distribute the traffic among the servers. To block a server from receiving server-to-server traffic, you must remove the server from the topology.

# Plan network requirements for Skype for Business

5/20/2019 • 19 minutes to read

**Summary:** Review the network component considerations below before implementing Skype for Business Server.

The information in these topics is also discussed in the whitepaper [Network Planning, Monitoring, and Troubleshooting with Lync Server](#) with additional details and depth. While the content refers explicitly to Lync 2010 and Lync 2013, the considerations for Skype for Business Server are unchanged.

Likewise, if your network involves wi-fi as well as wired access, the whitepaper [Delivering Lync 2013 Real-Time Communications over Wi-Fi](#) is a good reference and is equally applicable to Skype for Business Server.

## Server hardware

The network adapter of each server in the Skype for Business Server topology must support at least 1 gigabit per second (Gbps). In general, you should connect all server roles within the Skype for Business Server topology using a low latency and high bandwidth local area network (LAN). The size of the LAN depends on the size of the topology:

- In Standard Edition topologies, servers should be in a network that supports 1 Gbps Ethernet or equivalent.
- In Enterprise Edition topologies, most servers should be in a network that supports more than 1 Gbps, especially when supporting audio/video (A/V) conferencing and application sharing.

For public switched telephone network (PSTN) integration, you can integrate by using either T1/E1 lines or SIP trunking.

## Audio/Video network requirements

Network requirements for audio/video (A/V) in a Skype for Business Server deployment include the following:

- If you are deploying a single Edge Server or an Edge pool using DNS load balancing, you can configure the *external* firewall to perform network address translation (NAT). You can't configure the *internal* firewall to perform NAT. For details, see [Port and firewall planning](#).

### IMPORTANT

If you have an Edge pool and are using a hardware load balancer, you must use public IP addresses on the Edge Servers and you can't use NAT for the servers or the pool at your NAT-capable device (for example, a firewall appliance or LAN switch). For details, see [Edge Server scenarios in Skype for Business Server](#).

- If your organization uses a Quality of Service (QoS) infrastructure, the media subsystem is designed to work within this existing infrastructure.
- If you use Internet Protocol security (IPsec), we recommend disabling IPsec over the port ranges used for A/V traffic. For details, see [IPsec exceptions](#).

To provide optimal media quality, do the following:

- Provision the network links to support throughput of 65 kilobits per second (Kbps) per audio stream and 500 Kbps per video stream, if they are enabled, during peak usage periods. A two-way audio or video

session uses two streams, so a simple audio/phone connection will require 130Kbps to cover each stream. Video will likewise use 1000 Kbps total to carry an upstream and downstream connection.

- To cope with unexpected spikes in traffic and increased usage over time, Skype for Business Server media endpoints can adapt to varying network conditions and support three times the throughput for audio and video while still maintaining acceptable quality. Do not assume that this adaptability will mask the problem when a network is under-provisioned. In an under-provisioned network, the ability of the Skype for Business Server media endpoints to dynamically deal with varying network conditions (for example, temporary high packet loss) is reduced.
- For network links where provisioning is very costly and difficult, you may have to consider provisioning for a lower volume of traffic. In this scenario, let the elasticity of the Skype for Business Server media endpoints absorb the difference between the traffic volume and the peak traffic level, at the cost of some reduction in the voice quality. Also, there will be a decrease in the headroom otherwise available to absorb sudden peaks in traffic.
- For links that cannot be provisioned correctly in the short term (for example, a site that uses very poor WAN links), consider disabling video for certain users.
- Provision the network to guarantee a maximum end-to-end delay (latency) of 150 milliseconds (ms) under peak load. Latency is the one network impairment that Skype for Business Server media components can't reduce, and it is important to find and eliminate the weak points.
- For servers that are running antivirus software, include all servers that are running Skype for Business Server in the exception list to provide optimal performance and audio quality.

## IPsec exceptions

For enterprise networks where Internet Protocol security (IPsec) (see IETF RFC 4301-4309) has been deployed, IPsec must be disabled over the range of ports used for the delivery of audio, video, and panorama video. The recommendation is motivated by the need to avoid any delay in the allocation of media ports due to IPsec negotiation.

The following table explains the recommended IPsec exception settings.

### Recommended IPsec Exceptions

RULE NAME	SOURCE IP	DESTINATION IP	PROTOCOL	SOURCE PORT	DESTINATION PORT	AUTHENTICATI ON REQUIREMENT
A/V Edge Server Internal Inbound	Any	A/V Edge Server Internal	UDP and TCP	Any	Any	Do not authenticate
A/V Edge Server External Inbound	Any	A/V Edge Server External	UDP and TCP	Any	Any	Do not authenticate
A/V Edge Server Internal Outbound	A/V Edge Server Internal	A/V Edge Server External	UDP and TCP	Any	Any	Do not authenticate

<b>RULE NAME</b>	<b>SOURCE IP</b>	<b>DESTINATION IP</b>	<b>PROTOCOL</b>	<b>SOURCE PORT</b>	<b>DESTINATION PORT</b>	<b>AUTHENTICATI ON REQUIREMENT</b>
A/V Edge Server External Outbound	A/V Edge Server External	Any	UDP and TCP	Any	Any	Do not authenticate
Mediation Server Inbound	Any	Mediation Server(s)	UDP and TCP	Any	Any	Do not authenticate
Mediation Server Outbound	Mediation Server(s)	Any	UDP and TCP	Any	Any	Do not authenticate
Conferencing Attendant Inbound	Any	Front End Server running Conferencing Attendant	UDP and TCP	Any	Any	Do not authenticate
Conferencing Attendant Outbound	Front End Server running Conferencing Attendant	Any	UDP and TCP	Any	Any	Do not authenticate
A/V Conferencing Inbound	Any	Front End Servers	UDP and TCP	Any	Any	Do not authenticate
A/V Conferencing Outbound	Front End Servers	Any	UDP and TCP	Any	Any	Do not authenticate
Exchange Inbound	Any	Exchange Unified Messaging	UDP and TCP	Any	Any	Do not authenticate
Application Sharing Servers Inbound	Any	Application Sharing Servers	UDP and TCP	Any	Any	Do not authenticate
Application Sharing Server Outbound	Application Sharing Servers	Any	UDP and TCP	Any	Any	Do not authenticate
Exchange Outbound	Exchange Unified Messaging	Any	UDP and TCP	Any	Any	Do not authenticate
Clients	Any	Any	UDP and TCP	Any	Any	Do not authenticate



# Conferencing network requirements

The bandwidth used to download conference content from the Internet Information Services (IIS) server depends on the size of the content. You may choose to monitor the actual usage and adjust bandwidth planning accordingly.

## Network bandwidth requirements for media traffic

An important part of network planning is ensuring that your network can handle the media traffic generated by Skype for Business Server. This section helps you plan for that media traffic.

### Media traffic network usage

The media traffic bandwidth usage can be challenging to calculate because of the number of different variables, such as codec usage, resolution, and activity levels. The bandwidth usage is a function of the codec that is used and the activity of the stream, which can vary between scenarios. The following table lists the audio codecs typically used in Skype for Business Server scenarios.

### Audio codec bandwidth

AUDIO CODEC	SCENARIO	AUDIO PAYLOAD BIT RATE (KBPS)	BANDWIDTH AUDIO PAYLOAD AND IP HEADER ONLY (KBPS)	BANDWIDTH AUDIO PAYLOAD, IP HEADER, UDP, RTP AND SRTP (KBPS)	BANDWIDTH AUDIO PAYLOAD, IP HEADER, UDP, RTP, SRTP AND FORWARD ERROR CORRECTION (KBPS)
RTAudio Wideband	Peer-to-peer	29.0	45.0	57.0	86.0
RTAudio Narrowband	Peer-to-peer PSTN	11.8	27.8	39.8	51.6
G.722	Conferencing	64.0	80.0	95.6	159.6
G.722 Stereo	Peer-to-peer Conferencing	128.0	144.0	159.6	223.6
G.711	PSTN, Conferencing	64.0	80.0	92.0	156.0
Siren	Conferencing	16.0	32.0	47.6	63.6
SILK Wideband	Peer-to-peer	36.0	52.0	64.0	100.0
SILK Wideband	Peer-to-peer	26.0	42.0	54.0	80.0
SILK Wideband	Peer-to-peer	20.0	36.0	48.0	68.0
SILK wideband/narrow band	Peer-to-peer	13.0	29.0	41.0	54.0

## NOTE

PSTN calls from the Skype for Business client usually use the G.711 codec, which requires a high bandwidth. If enough bandwidth is not available for that codec, then calls can fail with an error that resembles the following in the Media logs: **At least one codec must be enabled, hr: c0042004**. Media logs (.blog files) are encrypted and can be decoded only by Microsoft support personnel.

The bandwidth numbers in the previous table are based on 20ms packetization (50 packets per second) and for the Siren and G.722 codecs include the additional secure real-time transport protocol (SRTP) overhead from conferencing scenarios and assume the stream is 100% active. Forward Error Correction (FEC) is used dynamically when there is packet loss on the link to help maintain the quality of the audio stream.

The stereo version of the G.722 codec is used by systems that are based on the Lync Room System, which uses a single stereo microphone or a pair of mono microphones to allow listeners to better distinguish multiple speakers in the meeting room.

## Video Resolution Bandwidth

VIDEO CODEC	RESOLUTION AND ASPECT RATIO	MAXIMUM VIDEO PAYLOAD BIT RATE (KBPS)	MINIMUM VIDEO PAYLOAD BIT RATE (KBPS)
H.264	320x180 (16:9) 212x160 (4:3)	250	15
H.264/RTVideo	424x240 (16:9) 320x240 (4:3)	350	100
H.264	480x270 (16:9) 424x320 (4:3)	450	200
H.264/RTVideo	640x360 (16:9) 640x480 (4:3)	800	300
H.264	848x480 (16:9)	1500	400
H.264	960x540 (16:9)	2000	500
H.264/RTVideo	1280x720 (16:9)	2500	700
H.264	1920x1080 (16:9)	4000	1500
H.264/RTVideo	960x144 (20:3)	500	15
H.264	1280x192 (20:3)	1000	250
H.264	1920x288 (20:3)	2000	500

The default codec for video is the H.264/MPEG-4 Part 10 Advanced Video Coding standard, together with its scalable video coding extensions for temporal scalability. To maintain interoperability with legacy clients, the RTVideo codec is still used for peer-to-peer calls between Skype for Business Server and legacy clients. In conference sessions with both Skype for Business Server and legacy clients the Skype for Business Server endpoint may encode the video using both video codecs and send the H.264 bitstream to the Skype for Business Server clients and the RTVideo bitstream to legacy clients.

The bandwidth required depends on the resolution, quality, frame rate, and the amount of motion or change in the

picture. For each resolution, there are two pertinent bit rates:

- **Maximum payload bit rate** This is the bit rate that an endpoint will use for resolution at the maximum frame rate. This is the value that allows the highest video and sound quality.
- **Minimum payload bit rate** This is the bit rate below which a Skype for Business Server endpoint will switch to the next lower resolution. To guarantee a certain resolution, the available video payload bit rate must not fall below this minimum bit rate for that resolution. This value helps you understand the lowest value possible if the maximum bit rate is not available or practical. For some users, such a low bit rate video might provide an unacceptable video experience so use caution with these minimum video payload bit rates. Note that for static, unchanging video scenes the actual bit rate may temporarily fall below the minimum bit rate.

Skype for Business Server supports many resolutions. This allows Skype for Business Server to adjust to different network bandwidth and receiving client capabilities. The default aspect ratio for Skype for Business Server is 16:9. The legacy 4:3 aspect ratio is still supported for webcams which don't allow capture in the 16:9 aspect ratio.

Video FEC is always included in the video payload bit rate when it is used so there are no separate values for with video FEC and without video FEC.

Endpoints do not stream audio or video packets continuously. Depending on the scenario there are different levels of stream activity which indicate how often packets are sent for a stream. The activity of a stream depends on the media and the scenario, and does not depend on the codec being used. In a peer-to-peer scenario:

- Endpoints only send audio streams when the users speak.
- Both participants receive audio streams.
- If video is used, both endpoints send and receive video streams during the call.
- For static video scenes the actual bit rate may temporarily be very low as the video codec will skip encoding regions of the video without a change since the prior sample.

In a conferencing scenario:

- Endpoints send audio streams only when the users speak.
- All participants receive audio streams.
- If video is used, all participants can receive up to five receive video streams and one panoramic (for example, aspect ratio 20:3) video stream. By default the five receive video streams are based on active speaker history but users can also manually select the participants from which they want to receive a video stream. If multi-video is enabled, the resolution and bandwidth requirement for each of the video streams will be lower.
- Each participant that turns on the user's send video stream will send one or more video streams. Skype for Business Server has the capability of sending up to five video streams to optimize the video quality for all the receiving clients. The actual number of video streams being sent is determined by the sender based on CPU capability, available uplink bandwidth, and the number of receiving clients requesting a certain video stream. The most common case is that one H.264 and one RTVideo video stream are being sent in case a legacy client joins the conference. Another common scenario is that several H.264 video streams (for example, with different video resolutions) are sent to accommodate different receiver requests.

In addition to the bandwidth required for the real-time transport protocol (RTP) traffic for audio and video media, bandwidth is required for real-time transport control protocol (RTCP). RTCP is used for reporting statistics and out-of-band control of the RTP stream. For planning, use the bandwidth numbers in the following table for RTCP traffic. These values represent the maximum bandwidth used for RTCP and are different for audio and video streams because of differences in the control data

## RTCP Bandwidth

MEDIA	RTCP MAXIMUM BANDWIDTH (KBPS)
Audio	5
Video (Only H.264 or RTVideo being sent/received)	10
Video (H.264 and RTVideo being sent/received)	15

For capacity planning, the following two statistics are of interest:

- Maximum bandwidth without FEC** The maximum bandwidth that a stream will consume. This includes the typical activity of the stream and the typical codec that is used in the scenario without FEC. This is the bandwidth when the stream is at 100% activity and there is no packet loss triggering the use of FEC. This is useful for computing how much bandwidth must be allocated to allow the codec to be used in a given scenario. FEC is not expected to be a requirement on a managed network.
- Maximum bandwidth with FEC** The maximum bandwidth that a stream consumes. This includes the typical activity of the stream and the typical codec that is used in the scenario with FEC. This is the bandwidth when the stream is at 100% activity and there is packet loss triggering the use of FEC to improve quality. This is useful for computing how much bandwidth must be allocated to allow the codec to be used in a given scenario and allow the use of FEC to preserve quality under packet-loss conditions.

The following tables also list an additional bandwidth value, **Typical bandwidth**. This is the average bandwidth that a stream consumes. This includes the typical activity of the stream and the typical codec that is used in the scenario. This bandwidth can be used for approximating how much bandwidth is being consumed by media traffic at a specific time, but should not be used for capacity planning, because individual calls will exceed this value when the activity level is greater than average. The typical video stream bandwidth in the tables below is based on a mix of different video resolutions as observed in measured customer data, and smaller installations are likely to have actual numbers that differ from the table data. For example, in peer-to-peer sessions most users would use the default video render window whereas some percentage of users would increase or maximize the Skype for Business Server application to allow better video resolutions.

The following tables provide values for the various scenarios.

### Audio/Video Capacity Planning for Peer-to-Peer Sessions

MEDIA	CODEC	TYPICAL STREAM BANDWIDTH (KBPS)	MAXIMUM STREAM BANDWIDTH WITHOUT FEC	MAXIMUM STREAM BANDWIDTH WITH FEC
Audio	RTAudio Wideband	39.8	62	91
Audio	RTAudio Narrowband	29.3	44.8	56.6
Audio	SILK Wideband	44.3	69	105
Main video when calling Skype for Business Server endpoints	H.264	460	4010 (for maximum resolution of 1920x1080)	Already included

MEDIA	CODEC	TYPICAL STREAM BANDWIDTH (KBPS)	MAXIMUM STREAM BANDWIDTH WITHOUT FEC	MAXIMUM STREAM BANDWIDTH WITH FEC
Main video when calling Lync 2010 or Office Communicator 2007 R2 endpoints	RTVideo	460	2510 (for maximum resolution of 1280x720)	Already included
Panoramic video when calling Skype for Business Server endpoints	H.264	190	2010 (for maximum resolution of 1920x288)	Already included
Panoramic video when calling Lync 2010 endpoints	RTVideo	190	510 (for maximum resolution of 960x144)	Already included

### Audio/Video Capacity Planning for Conferences

MEDIA	TYPICAL CODEC	TYPICAL STREAM BANDWIDTH (KBPS)	MAXIMUM STREAM BANDWIDTH WITHOUT FEC	MAXIMUM STREAM BANDWIDTH WITH FEC
Audio	G.722	46.1	100.6	164.6
Audio	Siren	25.5	52.6	68.6
Main video receive	H.264 and RTVideo <sup>1</sup>	260	8015	Not applicable
Main video send	H.264 and RTVideo	270	8015	Not applicable
Panoramic video receive	H.264 and RTVideo	190	2010 (for maximum resolution of 1920x288)	Not applicable
Panoramic video send	H.264 and RTVideo	190	2515 <sup>2</sup>	Not applicable

1. RT Video is sent in addition to H.264 when Lync 2010 clients are connected to the conference.
2. If there are multiple streams, they dynamically share the allocated bandwidth.

For the main video the typical stream bandwidth is the aggregated bandwidth over all received video streams and the maximum stream is the bandwidth over all send video streams. Even with multiple video streams the typical video bandwidth is smaller than in the peer-to-peer scenario because many video conferences are using content sharing that leads to much smaller video windows and therefore smaller video resolutions. The maximum supported aggregated video payload bandwidth is 8000 Kbps for both, send and receive streams which would be used (e.g. if there are two incoming 1920x1080p video streams). Maximum values are only rarely seen in actual implementations.

When building out a multiparty conference that uses the gallery view feature, bandwidth utilization increases initially as participants join, then decreases as resolutions are dropped to fit within the maximum.

	2 PARTICIPANTS	3 PARTICIPANTS	4 PARTICIPANTS	5 PARTICIPANTS	6 PARTICIPANTS
<b>Max resolutions received</b>	1920x1080	1280x720	640x360	640x360 320x240	640x360 320x240

	2 PARTICIPANTS	3 PARTICIPANTS	4 PARTICIPANTS	5 PARTICIPANTS	6 PARTICIPANTS
<b>Total average bit rate</b>	2128	4050	1304	1224	1565
<b>Total Maximum bit rate</b>	4063	5890	2860	2699	3017

The typical stream bandwidth for panoramic video is based on devices that only stream up to 960x144 panoramic video. Expect the typical stream bandwidth to increase when using devices with 1920x288 panoramic video.

### Audio Capacity Planning for PSTN

MEDIA	TYPICAL CODEC	TYPICAL STREAM BANDWIDTH (KBPS)	MAXIMUM STREAM BANDWIDTH WITHOUT FEC	MAXIMUM STREAM BANDWIDTH WITH FEC
Audio	G.711 (this includes PSTN participants in conferences)	64.8	97	161
Audio	RTAudio Narrowband	30.9	44.8	56.6

The network bandwidth numbers in these tables represent one-way traffic only and include 5 Kbps for RTCP traffic overhead for each stream.

## Managing Quality of Service

Quality of Service (QoS) is a networking technology that is used in some organizations to help provide an optimal end-user experience for audio and video communications. QoS is most frequently used on networks where bandwidth is limited: with a large number of network packets competing for a fairly small amount of available bandwidth, QoS enables administrators to assign higher priorities to packets carrying audio or video data. By giving these packets a higher priority, audio and video communications are likely to complete faster, and with less interruption, than network sessions involving things such as file transfers, web browsing, or database backups. That's because network packets used for file transfers or database backups are assigned a "best effort" priority.

#### NOTE

As a rule, QoS applies only to communication sessions on your internal network. When you implement QoS, you configure your servers and routers to support packet marking in a particular manner that may not be supported on the Internet or on other networks. Even if Quality of Service is supported on other networks, there is no guarantee that QoS will be configured in exactly the same way you configured the service. If you are using MPLS, you'll need to work with your MPLS provider.

Skype for Business Server does not require QoS, but it is strongly recommended. If you experience packet loss issues on the network your available solutions are to add more bandwidth or to implement QoS. If adding more bandwidth is not possible, then implementing QoS might be your only toll to resolve the problem.

Skype for Business Server offers full support for QoS: that means that organizations that are already using QoS can easily integrate Skype for Business Server into their existing network infrastructure. To do this you must follow these steps:

- [Enabling QoS in Skype for Business Server for devices that are not based on Windows](#). By default, QoS is disabled for computers and other devices (such as iPhones) that run other operating systems. Although you can use Skype for Business Server to enable and disable Quality of Service for devices, you typically cannot

use the product to modify the DSCP codes used by these devices.

- [Configuring port ranges and a Quality of Service policy for your Conferencing, Application, and Mediation servers](#). You must reserve a unique set of ports for different packet types, such as audio and video. By using Skype for Business Server you do not enable or disable QoS by setting a property value to True or to False. Instead, you enable QoS by configuring port ranges and then creating and applying Group Policy. If you later decide not to use QoS you can "disable" QoS by removing the appropriate Group Policy objects.
- [Configuring port ranges and a Quality of Service policy for your Edge Servers](#). Although not required, you can configure your Edge servers to use the same port ranges as your other servers. Configuring a QoS policy only be done for the internal side of your Edge servers. That's because QoS is designed for use on your internal network and not on the Internet.
- [Configuring port ranges and a Quality of Service policy for your clients in Skype for Business Server](#). These port ranges apply only to client computers and are typically different from the port ranges configured on your servers. Note that Skype for Business Server does not support QoS for Windows operating systems other than Windows 10.

#### **NOTE**

If you are using Windows Server 2012 or Windows Server 2012 R2 you might be interested in the new set of Windows PowerShell cmdlets available for managing QoS on that platform. For more information, see [Network QoS Cmdlets in Windows PowerShell](#).

QoS is also discussed in the whitepaper [Network Planning, Monitoring, and Troubleshooting with Lync Server](#) with additional details and depth. While the content refers explicitly to Lync 2010 and Lync 2013, the considerations for Skype for Business Server are unchanged.

## See also

[Plan for IPv6 in Skype for Business](#)

[Load balancing requirements for Skype for Business](#)

[DNS requirements for Skype for Business Server](#)

# Plan for IPv6 in Skype for Business

5/20/2019 • 7 minutes to read

**Summary:** Implement IPv6 before you install Skype for Business Server.

Skype for Business Server includes support for IP version 6 (IPv6) addresses, along with continued support of IP version 4 (IPv4) addresses.

IPv4 addresses are 32-bit addresses that allow a computer to communicate over the Internet. Due to the increasing number of devices worldwide, the available IPv4 addresses have run out. Because of this, many new devices are moving to using IPv6 addresses. IPv6 addresses perform the same function as IPv4 addresses (with some additional features), but instead of using only 32-bits, IPv6 addresses use 128-bits. This provides not only a new set of addresses, but also a much larger number of them.

A typical IPv4 address looks something like this: 192.0.2.235, whereas an IPv6 address looks like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. The change in formatting and functionality for devices that use IPv6 addresses requires several deployment and configuration considerations in your Skype for Business Server installation.

This topic includes the following sections:

- [Overview of IP address types](#)
- [Technical requirements for IPv6](#)
- [Migration and coexistence considerations for IPv6](#)

If you determine you will be using IPv6 addresses, refer to the [Configure IP address types in Skype for Business](#) article.

## Overview of IP address types

You have three options when configuring IP addresses in Skype for Business Server. You can configure Skype for Business Server to support only IP version 4 (IPv4), only IP version 6 (IPv6), or a combination of both (known as a dual stack). There are several issues to consider with each type of configuration:

- **IPv4 only** IPv6 was created because the world is running out of IPv4 addresses. Ultimately, IPv6 will be fully supported worldwide, but at this time, many companies and devices that your enterprise might need to communicate with do not yet support IPv6, and may not for some time. An IPv4-only configuration will help to ensure that your Skype for Business Server implementation can communicate with most existing devices.
- **IPv6 only** Conversely, a full IPv6 implementation will exclude communication with many existing devices.
- **Dual Stack** Dual stack is a network where both IPv4 and IPv6 addresses are enabled. This configuration is supported in Skype for Business Server because in most cases the transition from full-IPv4 to full-IPv6 will take several years.

The following sections outline the compatibility among these three configurations for various Skype for Business Server features.



**NOTE**

Client or server configuration with IPv6 only is supported only for lab or validation purposes. IPv6 only configuration is not supported in the production deployment.

**Client Registration**

CLIENT ENDPOINT NETWORK	SERVER NETWORK
IPv4	IPv4
IPv4	Dual stack
Dual stack	IPv4
Dual stack	Dual stack
Dual stack	IPv6
IPv6	Dual stack
IPv6	IPv6

**Peer-to-Peer Client**

Peer-to-peer communications include audio, audio/video, application sharing, and file transfer. After both clients have successfully registered, the following combinations are supported.

CLIENT ENDPOINT 1	CLIENT ENDPOINT 2
IPv4	IPv4
IPv4	Dual stack
Dual stack	Dual stack
IPv6	Dual stack
IPv6	IPv6

**Conferencing**

Conferencing includes audio/video, application sharing, and data collaboration applications like whiteboarding and file sharing.

CLIENT ENDPOINT NETWORK	SERVER NETWORK
IPv4	IPv4
IPv4	Dual stack
Dual stack	IPv4

CLIENT ENDPOINT NETWORK	SERVER NETWORK
Dual stack	Dual stack
Dual stack	IPv6
IPv6	Dual stack
IPv6	IPv6

### Mediation Server/PSTN

Skype for Business Server does not support media bypass for public switched telephone network (PSTN) calls if the traffic is through an IPv6 interface. If media bypass is required, we recommend that the PSTN gateway is configured to IPv4.

PRIMARY INTERFACE 1	PSTN INTERFACE (ON MEDIATION SERVER)	PSTN GATEWAY SETTING
IPv4	Dual stack	IPv4
Dual stack	Dual stack	IPv4
Dual stack	Dual stack	IPv6

1. The primary interface is the interface that communicates with the Skype for Business Server components.

### Remote User Peer-to-Peer Communications

Peer-to-peer communications with remote users include instant messaging, audio/video, application sharing, and file transfer.

REMOTE USER NETWORK	EDGE SERVER (EXTERNAL EDGE)
IPv4	IPv4
Dual stack	IPv4
Dual stack	Dual stack
IPv6	Dual stack
IPv6	IPv6

### Front End Pool and Edge Pool Configuration

The following table shows the support matrix between the Front End Server pool and the internal Edge Server pool.

#### Front End Pool and Edge Pool (Internal Edge) Matrix

	EDGE POOL: IPV4	EDGE POOL: DUAL STACK	EDGE POOL: IPV6
<b>Front End Pool: IPv4</b>	Yes	Yes	No
<b>Front End Pool: Dual Stack</b>	Yes	Yes	No

	EDGE POOL: IPV4	EDGE POOL: DUAL STACK	EDGE POOL: IPV6
<b>Front End Pool: IPv6</b>	No	No	Yes*

\* Use this combination only in a lab environment.

The following table is a matrix of the supported combinations of internal and external edge interfaces.

### Edge Pool (Internal Edge) and Edge pool (External Edge) Matrix

	EDGE POOL (EXTERNAL EDGE) : IPV4	EDGE POOL (EXTERNAL EDGE): DUAL STACK	EDGE POOL (EXTERNAL EDGE): IPV6
<b>Edge Pool (Internal Edge): IPv4</b>	Yes	Yes	No
<b>Edge Pool (Internal Edge): Dual Stack</b>	No	Yes	No
<b>Edge Pool (Internal Edge): IPv6</b>	No	No	Yes*

\* Use this combination only in a lab environment.

### Advanced Enterprise Voice Support for IPv6

Deployments that include call admission control (CAC), Enhanced 9-1-1 (E9-1-1), or media bypass must be configured as IPv4 only or as a dual-stacked implementation. Endpoints using only IPv6 cannot use any of these features.

#### NOTE

In a dual-stacked deployment, even if a Skype for Business Server client connects to a Skype for Business Server by using IPv6, Skype for Business Server will make a best effort to map an appropriate IPv4 address to support E9-1-1.

Location Information service with IPv6 addresses is not supported.

Exchange Unified Messaging (UM) does not support IPv6. For Exchange UM, be sure that DNS resolution does not return an IPv6 address. Using IPv6 may cause failure when calls are sent to voice mail.

### Other Skype for Business Server Feature Support for IPv6

In addition to the features and components mentioned previously, Skype for Business Server supports IPv6 for the following features:

- **Persistent Chat**

You configure IPv6 for Persistent Chat by using Topology Builder. For details about configuring Persistent Chat, see the Deploying Persistent Chat Server documentation.

- **Quality of Experience (QoE) and call detail recording (CDR) reports**

Monitoring reports include the IP address as it is stored in the Monitoring Server database, whether of type IPv4 or IPv6.

## Technical requirements for IPv6

If you plan to configure Skype for Business Server for IPv6, keep the following requirements in mind:

- To use IPv6 addresses with Skype for Business Server, you need to create domain name system (DNS) records for records that must be discovered and resolved to an IPv6 address. IPv6 DNS uses host AAAA (quad-A) records. If you use both IPv4 and IPv6 in your deployment, it is best to configure and maintain both host A records for IPv4 and host AAAA records for IPv6. Even when you fully transition your deployment to IPv6, you may still require IPv4 DNS host records for external users who still use IPv4.

You can deploy IPv6 DNS host records before you start using IPv6. If the client or server doesn't use IPv6, the record will not be referenced. Transitional technologies will make the decision about which record to use, based on transition technology configuration and policies.

- Each IPv6 address has a scope. The three scopes that you can use for IPv6 addressing are IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges), and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4). All the servers within a pool should have IPv6 addresses with the same scope.

#### **IMPORTANT**

IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to help ensure that the addresses that you assign at the Windows Server level and at the Skype for Business Server level work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.

## Migration and coexistence considerations for IPv6

IP version 6 (IPv6) is not supported on Lync Server 2010 or Office Communications Server. For piloting purposes, you can test Lync Server 2010 and Skype for Business Server dual-stack coexistence. We recommend that all pools for a given central site are upgraded to Skype for Business Server before you enable IPv6 (dual-stack network) for any of the pools. If you need to configure a pool for IPv6 only, we recommend that you set up an IPv6-only pool in your lab environment for testing.

The following scenarios are supported during migration and coexistence:

- Skype for Business Server, Lync Server 2013, and Lync Server 2010 pools in IPv4 mode, coexisting with Skype for Business Server in dual-stack mode.
- Skype for Business Server pool in IPv6-only mode, if the IPv6-only pool is siloed.

## See also

[Configure IP address types in Skype for Business](#)

[IP Version 6 Addressing Architecture](#)

[IPv6 Global Unicast Address Format](#)

[Unique Local IPv6 Unicast Addresses](#)

# Configure IP address types in Skype for Business

5/20/2019 • 3 minutes to read

**Summary:** Review the IP Address type considerations below before implementing Skype for Business Server.

You deploy IP address types by using topology settings that you configure in Topology Builder. This section describes how to deploy IP address types on Front End Servers, Mediation Servers, and Edge Servers.

## Deploy IP address types on a Front End Server

Using Topology Builder, perform the steps in the following procedure to deploy IP address types on a Front End Server.

### To deploy IP address types on a Front End Server

1. Under **Enterprise Edition Front End pools**, right-click the server within a pool, and then select **Edit Properties**. (Alternatively, select the server, and then click **Edit Properties** from the **Action** menu.)
2. In the **Edit Properties** dialog box, select the IP address type that you want to configure. For a dual-stack configuration, select **Enable IPv4** and **Enable IPv6**.

### Edit Properties dialog box for the Front End Server pool

- **Use all configured IP addresses.** Select this option if you want to allow any IP address defined on the computer to be used.

#### NOTE

This is the recommended option for IP version 6 (IPv6) configurations.

- **Limit service usage to selected IP addresses.** Select this option to specify a specific address to use on the new server. If you select this option, you must enter a value for **Primary IP address**.
- **Primary IP address.** Enter an IP address that the server will use for all communications except public switched telephone network (PSTN). The IP address entered must match the format of the select address type.
- **PSTN IP address.** Define a PSTN IP address when a Mediation Server is collocated on the Front End Server. This address must match the format of the selected address type.

#### NOTE

The installation of additional network interface cards (NICs) to support the PSTN IP address configuration (or for any other reason) on Front End Servers is not supported. For more information about supported NIC configurations for Skype for Business Server, see [Server hardware platforms for Lync Server 2013](#).

## Deploy IP address types on a Mediation Server

Using Topology Builder, perform the steps in the following procedure to deploy IP address types on a Mediation Server.

### To deploy IP address types on a Mediation Server

- In Topology Builder, under **Mediation pools**, right-click the server within a pool, and then select **Edit Properties**. (Alternatively, select the server, and then click **Edit Properties** from the **Action** menu.)
- In the **Edit Properties** dialog box, select the IP address type that you want to configure. For a dual-stack configuration, select **Enable IPv4** and **Enable IPv6**, as shown in the following figure.

#### **Edit Properties dialog box for the Mediation Server pool**

- **Use all configured IP addresses.** Select this option if you want to allow any IP address defined on the computer to be used.

#### **NOTE**

This is the recommended option for IP version 6 (IPv6) configurations.

- **Limit service usage to selected IP addresses.** Select this option to specify a specific address to use on the new server. If you select this option, you must enter a value for Primary IP address.
- **Primary IP address.** Enter an IP address that the server will use for all communications except public switched telephone network (PSTN). The IP address entered must match the format of the select address type.
- **PSTN IP address.** Define a PSTN IP address when a Mediation Server is collocated on the Front End Server. This address must match the format of the selected address type.

#### **IMPORTANT**

We only support two network cards on *dedicated* Mediation Servers. If the Mediation Sserver role is collocated on the Front End, then dual network cards are not supported.

#### **NOTE**

- For more information about supported NIC configurations for Skype for Business Server 2015, see [Hardware for Skype for Business Server 2015](#)
- For more information about supported NIC configurations for Skype for Business Server 2019, see [Hardware for Skype for Business Server 2019](#)

## Deploy IP address types on an Edge Server

Using Topology Builder, perform the following steps:

#### **To deploy IP address types on an Edge Server**

1. In Topology Builder, under **Edge pools**, right-click the server within a pool, and then select **Edit Properties**. (Alternatively, select the server, and then click **Edit Properties** from the **Action** menu.)
2. In the **Edit Properties** window, select the IP address configuration that you want to support.
3. For each address type that you select, you must supply appropriate internal and external addresses.

# DNS requirements for Skype for Business Server

6/25/2019 • 14 minutes to read

**Summary:** Review the DNS considerations in this topic before implementing Skype for Business Server.

This article only addresses DNS planning for Skype for Business Server deployments on an organization's on-premise network. For Skype for Business Online refer to "Office 365 URLs and IP address ranges" at <https://aka.ms/o365ips>.

A Domain name service (DNS) server maps hostnames (like [www.contoso.com](http://www.contoso.com), presumably a web server) to IP addresses (such as 10.10.10.10). It helps clients and interdependent servers communicate with each other on the network. When you set up an implementation of Skype for Business Server 2015 you'll need to make sure the mapping of new server names (usually reflecting the role they'll be taking on) matches the IP addresses they are assigned to.

While this may seem a bit daunting at first, the heavy lifting for planning this can be done using the [Skype for Business Server 2015 Planning Tool](#). Once you've gone through the wizard's questions about what features you plan to use, for each site you define you can view the DNS Report within the Edge Admin Report, and use the information listed there to create your DNS records. You can also make adjustments to many of the names and IP addresses used, for details see [Review the DNS Report](#). Keep in mind you can export the Edge Admin Report to an Excel spreadsheet, and the DNS Report will be one of the worksheets in the file. While this tool includes features [deprecated from Skype for Business Server 2019](#), it can still be used to create an initial plan if those features are not selected

When you are installing a new implementation as described in [Create DNS records for Skype for Business Server](#) and building your topology for Skype for Business Server, we recognize that you can choose to use the DNS capabilities built in to Windows Server 2016 or a third-party DNS package, so we'll keep the discussions in this article general rather than specific. We're detailing what's needed, and how you meet that need is your decision to make.

Experienced Skype for Business, Lync, and Office Communications Suite administrators will probably find the following tables useful. If the table is confusing to you, the later sections or articles will shed some light on the following concepts:

## Summary tables

The following tables show DNS records Skype for Business Server uses to provide services to users. Some are optional in that they are only needed to support certain features, and they can be skipped if those features are not desired. The DNS records needed for internal access only are in the first table, and a deployment allowing internal and external access will need records from both tables.

### Internal DNS mappings

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
-------------	-------	-------------	---------	----------

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
A/AAAA	Front End pool FQDN <i>FE-pool.contoso.com</i>	Front End pool server IP addresses DNS LB to <i>192.168.21.122</i> <i>192.168.21.123</i> <i>192.168.21.124</i>	DNS Load Balancing of Front End Pools. Maps the Front End pool name to a set of IP addresses. See <a href="#">Deploying DNS Load Balancing on Front End Pools and Director Pools</a>	Y
A/AAAA	FQDN of each Front End Server or Standard Edition server in a pool, or a standalone server <i>FE01.contoso.com</i> <i>FE02.contoso.com</i> <i>FE03.contoso.com</i>	Corresponding IP of each server <i>192.168.21.122</i> <i>192.168.21.123</i> <i>192.168.21.124</i>	Maps the server name to its IP address.	Y
A/AAAA	Enterprise Pool Internal Web Services Override FQDN <i>Web-int.contoso.com</i>	HLB VIP for Front End Server Internal Web Services <i>192.168.21.120</i>	Required to enable client to server web traffic, such as downloading the Skype for Business Web App. Also required for Mobile clients.	Y
A/AAAA	Enterprise Pool External Web Services Override FQDN <i>Web-ext.contoso.com</i>	HLB VIP for Front End Server External Web Services <i>68.123.56.90</i>	Required to enable client to server web traffic, such as downloading the Skype for Business Web App. Required if mobile clients will resolve DNS internally. Can resolve to DMZ Reverse Proxy IP or Internet IP.	
A/AAAA	Back End Server SQL server FQDN <i>SQL1.contoso.com</i>	server IP address <i>192.168.11.90</i>	Maps the server name for a back-end SQL server working with the Front End pool to its IP address	
A/AAAA	Back End Server Mirror SQL server FQDN <i>SQL2.contoso.com</i>	server IP address <i>192.168.11.91</i>	Maps the server name for a back-end SQL mirror server working with the Front End pool to its IP address	



RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
A/AAAA	Director pool FQDN <b>Note:</b> Not applicable when using a standalone Director server <i>DirPool.contoso.com</i>	Director pool IP addresses DNS LB to <i>192.168.21.132</i> , <i>192.168.21.133</i> , <i>192.168.21.134</i>	DNS load balancing of Director Pool servers. Maps the pool name for the Director pool to an IP address, see <a href="#">Deploying DNS Load Balancing on Front End Pools and Director Pools</a> A Director can authenticate a user and is optional.	
A/AAAA	Director FQDN	Server IP address of each Director server	Maps the pool name for the Director to an IP address, see <a href="#">Deploying DNS Load Balancing on Front End Pools and Director Pools</a>	
A/AAAA	Mediation Server pool FQDN	Pool IP addresses	The Mediation Server role is optional. You can co-locate the services provided by a mediation server to the Front End server or pool. See <a href="#">Using DNS Load Balancing on Mediation Server Pools</a>	
A/AAAA	Mediation Server FQDN	Server IP address	You can co-locate the services provided by a mediation server to the Front End server or pool. See <a href="#">Using DNS Load Balancing on Mediation Server Pools</a>	
A/AAAA	Persistent Chat Server FQDN	Persistent Chat Server IP address	A Persistent Chat server is required for the Persistent Chat feature and is otherwise optional.	

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
A/AAAA	lyncdiscoverinternal.< sipdomain> lyncdiscoverinternal.c ontoso.com	HLB Front End pool VIP or Director IP 192.168.21.121	Internal AutoDiscover Service1, required for Mobility support. If internal DNS is used to resolve for mobile devices, it should point to the external IP, or DMZ VIP. For Web services we require HLB on the Front End pool as HTTPS can't leverage DNS. For Front End pool or Director pool this should resolves to an HLB VIP, or a regular IP for a Standard edition server or a Standalone Director server.	Y
CNAME	lyncdiscoverinternal.< sipdomain> lyncdiscoverinternal. contoso.com	HLB FE Pool FQDN or Director FQDN Web-int.contoso.com	Internal AutoDiscover Service1 You can implement this as a CNAME instead of an A record if desired.	
A/AAAA	sip.<sipdomain> sip.contoso.com	Front End pool server IP addresses (or to a each Director IP address) DNS LB to 192.168.21.122 192.168.21.123 192.168.21.124	Required for automatic configuration, see <a href="#">Walkthrough of Skype for Business clients locating services</a> A record or records pointing to the Front End pool servers or Director servers on the internal network, or the Access Edge service when the client is external	2
A/AAAA	ucupdates- r2.<sipdomain> ucupdates- r2.contoso.com	HLB FE Pool VIP Or Director Pool HLB VIP , or SE/Director Server IP 192.168.21.121	Deploying this record is optional 3	
SRV	_sipinternaltls._tcp.<si pdomain> Port 5061 _sipinternaltls._tcp.co ntoso.com Port 5061	Front End pool FQDN FE-Pool.contoso.com	Enables Internal user automatic sign-in 1 to the Front End server/pool or SE server/pool that authenticates and redirects client requests for sign-in.	2

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
A/AAAA	sipinternal.<sipdomain> sipinternal.contoso.com	Front End pool FQDN FE-Pool.contoso.com	Internal user access <b>1</b>	<b>2</b>
SRV	_ntp_udp.<sipdomain> _ntp_udp.contoso.com	TimeServer FQDN north-america.pool.ntp.org	NTP source required for Lync Phone Edition devices	This is required to support desktop handsets.
SRV	_sipfederationtls_tcp.<sipdomain> _sipfederationtls_tcp.contoso.com	Access Edge service FQDN EdgePool-int.contoso.com	Create one SRV record for each SIP domain that has IOS or Windows phone Mobile clients.	For Mobile client support
A/AAAA	admin URL Web-int.contoso.com	HLB FE Pool VIP 192.168.21.121	Skype for Business Server Control Panel, see <a href="#">Simple URLs</a>	
A/AAAA	meet URL Web-int.contoso.com	HLB FE Pool VIP 192.168.21.121	Online meetings, see <a href="#">Simple URLs</a>	
A/AAAA	dial-in URL Web-int.contoso.com	HLB FE Pool VIP 192.168.21.121	Dial-in conferencing, see <a href="#">Simple URLs</a>	
A/AAAA	internal Web Services FQDN Web-int.contoso.com	HLB FE Pool VIP 192.168.21.121	Skype for Business Web Service used by Skype for Business Web App	
A/AAAA	Office Web Apps Server pool FQDN OWA.contoso.com	Office Web Apps Server pool VIP address 192.168.1.5	Defines the Office Web Apps Server pool FQDN	
A/AAAA	Internal Web FQDN Web-int.contoso.com	Front End pool VIP address 192.168.21.121	Defines the Internal Web FQDN used by Skype for Business Web App If you are using DNS load balancing on this pool, your Front End pool and internal web farm cannot have the same FQDN.	

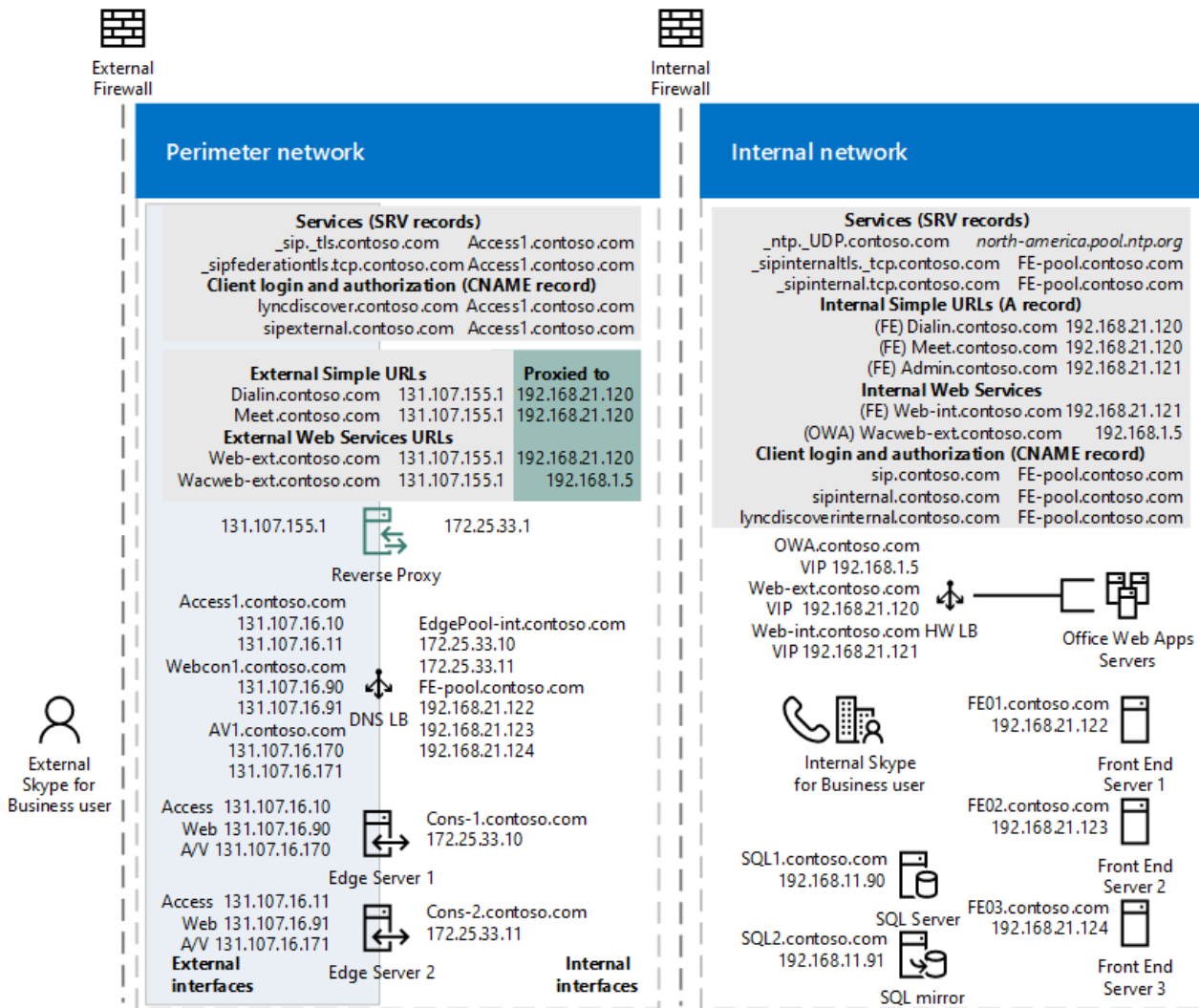
**1** Used by a client to discover the Front End Server or Front End pool, and be authenticated and signed in as a user. More detail on this is in [Walkthrough of Skype for Business clients locating services](#).

**2** This is only required to support legacy clients prior to Lync 2013, and desktop handsets.

**3** In the situation where a Unified Communications device is turned on, but a user has never logged into the device, the A record allows the device to discover the server hosting Device Update Web service and obtain updates. Otherwise, devices obtain the server information through in-band provisioning the first time a user logs in.

The following diagram shows an example that includes both internal and external DNS records, and many of the records shown in the surrounding tables:

### Edge network diagram using Public IPv4 addresses



### Perimeter network DNS mappings (both internal and external interfaces)

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
A/AAAA	Internal Edge pool FQDN <i>EdgePool-int.contoso.com</i>	Internal-facing Edge pool IP addresses 172.25.33.10, 172.25.33.11	Consolidated Edge Pool internal interface IP Addresses	Y
A/AAAA	Edge Server FQDN <i>Cons-1.contoso.com</i>	Internal-facing server IP for a server in the Edge pool 172.25.33.10	Create a record for each server in the pool with the server FQDN pointing to its internal server node IP in the pool, see <a href="#">DNS Load Balancing on Edge Server Pools</a> .	Y

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
A/AAAA	Access Edge service Pool FQDN <i>Access1.contoso.com</i>	Access Edge service Pool external IP addresses 131.107.16.10, 131.107.16.11	The Access Edge service provides a single, trusted connection point for both outbound and inbound Session Initiation Protocol (SIP) traffic.	Y
A/AAAA	Web Conferencing Edge service Pool FQDN <i>Webcon1.contoso.com</i>	Web Conferencing Edge service external IP addresses 131.107.16.90, 131.107.16.91	The Web Conferencing Edge service enables external users to join meetings that are hosted on your internal Skype for Business Server environment.	Y
A/AAAA	<i>av.&lt;sip-domain&gt;</i> Pool FQDN <i>AV1.contoso.com</i>	A/V Edge external IP addresses 131.107.16.170, 131.107.16.171	The A/V Edge service makes audio, video, application sharing and file transfer available to external users.	Y
CNAME	<i>sip.&lt;sipdomain&gt;</i> <i>sip.contoso.com</i>	External Access Edge Pool FQDN <i>Access1.contoso.com</i>	Locates the Edge Server pool . See <a href="#">Walkthrough of Skype for Business clients locating services</a>	Y
SRV	<i>_sip._tls.&lt;sipdomain&gt;</i> <i>_sip._tls.contoso.com</i>	External Access Edge FQDN <i>Access1.contoso.com</i>	Used for external user access. See <a href="#">Walkthrough of Skype for Business clients locating services</a>	Y
SRV	<i>_sipfederationtls._tcp.&lt;sipdomain&gt;</i> <i>_sipfederationtls._tcp.contoso.com</i>	External Access Edge FQDN <i>Access1.contoso.com</i>	Used for Federation and public IM connectivity	①
SRV	<i>_xmpp-server._tcp.&lt;sipdomain&gt;</i> <i>_xmpp-server._tcp.contoso.com</i>	External Access Edge FQDN <i>Access1.contoso.com</i>	The XMPP Proxy service accepts and sends extensible messaging and presence protocol (XMPP) messages to and from configured XMPP Federated partners.	Y, to deploy Federation, otherwise optional Not available in Skype for Business Server 2019.

RECORD TYPE	VALUE	RESOLVES TO	PURPOSE	REQUIRED
SRV	_sipfederationtls._tcp.<sipdomain> _sipfederationtls._tcp.contoso.com	External Access Edge FQDN Access 1.contoso.com	To support Push Notification Service and Apple Push Notification service, you create one SRV record for each SIP domain. 3	
A/AAAA	External Front End pool web services FQDN Web-ext.contoso.com	Reverse proxy public IP address, proxies to the External Web Services VIP for your Front End pool 1 131.107.155.1 proxy to 192.168.21.120	Front End pool external interface used by Skype for Business Web App	Y
A/AAAA/CNAME	lyncdiscover.<sipdomain> lyncdiscover.contoso.com	Reverse proxy public IP address, resolves to the External Web Services VIP for your Director pool, if you have one, or for your Front End pool if you do not have a Director 2 131.107.155.1 proxy to 192.168.21.120	External record for client AutoDiscover, also used by Mobility, Skype for Business Web App, and scheduler Web app, resolved by the reverse proxy server To support Push Notification Service and Apple Push Notification service, you create one SRV record for each SIP domain that has Microsoft Lync Mobile clients. 3	Y
A/AAAA	meet.<sipdomain> meet.contoso.com	Reverse proxy public IP address, resolves to the external Web interface for the Front End pool 131.107.155.1 proxy to 192.168.21.120	Proxy to Skype for Business Web Service See <a href="#">Simple URLs</a>	Y
A/AAAA	dial-in.<sipdomain> dial-in.contoso.com	Reverse proxy public IP address, proxies to the external Web interface for the Front End pool 131.107.155.1 proxy to 192.168.21.120	Proxy to Skype for Business Web Service See <a href="#">Simple URLs</a>	Y
A/AAAA	Office Web Apps Server pool FQDN OWA.contoso.com	Reverse proxy public IP address, proxies to the external Web interface for the Office Web Apps Server 131.107.155.1 proxy to 192.168.1.5	Office Web Apps Server pool VIP address 192.168.1.5	Defines the Office Web Apps Server pool FQDN

- 1 Required to deploy Federation, otherwise optional.
- 2 Used by a client to discover the front end server or Front End pool, and be authenticated and signed in as a user.
- 3 This requirement applies only to clients on Apple or Microsoft based mobile devices. Android and Nokia Symbian devices do not use push notification.

For more detail on Edge Servers and perimeter networks, see the Edge server [DNS planning](#) content.

#### IMPORTANT

Skype for Business Server supports the use of IPv6 addressing. See [Plan for IPv6 in Skype for Business](#) for more details.

#### IMPORTANT

For more detail on FQDNs, see [DNS basics](#).

## Split brain DNS

Split brain DNS is a DNS configuration where you have two DNS zones with the same namespace. The first DNS zone handles internal requests, while the second DNS zone handles external requests, as mentioned in these tables. For more about this see [Split-brain DNS](#).

## Hybrid considerations

If you plan to have some users homed online and some homed on premises, refer to the Hybrid connectivity planning article [Skype for Business server 2019](#). You will need to configure DNS as normal for Skype for Business Server 2015 and also add additional DNS records.

You should also refer to "Office 365 URLs and IP address ranges" at <https://aka.ms/o365ips> to confirm that your users will have access to the online resources they will need.

## Simple URLs

A Uniform Resource Locator (URL) is a reference to a web resource that specifies its location on a computer network and a protocol used to retrieve it.

Skype for Business Server supports using three "simple" URLs to access services:

- **Meet** is used as the base URL for all conferences in the site. An example of a Meet simple URL is <https://meet.contoso.com>. A URL for a particular meeting might be <https://meet.contoso.com/username/7322994>.

With the Meet simple URL, links to join meetings are easy to comprehend and easy to communicate.

- **Dial-in** enables access to the Dial-in Conferencing Settings web page. This page displays conference dial-in numbers with their available languages, assigned conference information (that is, for meetings that do not need to be scheduled), and in-conference DTMF controls, and supports management of personal identification number (PIN) and assigned conferencing information. The Dial-in simple URL is included in all meeting invitations so that users who want to dial in to the meeting can access the necessary phone number and PIN information. An example of the Dial-in simple URL is <https://dialin.contoso.com>.
- **Admin** enables quick access to the Skype for Business Server Control Panel. From any computer within your organization's firewalls, an admin can open the Skype for Business Server Control Panel by typing the Admin simple URL into a browser. The Admin simple URL is internal to your organization. An example of

the Admin simple URL is <https://admin.contoso.com>.

Simple URLs are discussed in more detail at [DNS requirements for simple URLs in Skype for Business Server](#).

## DNS by server role

You can set the names of these pools and servers as you wish, but make them memorable and reflect their function in the system.

### DNS records for individual servers or pools

These generic record requirements apply to any server role used by Skype for Business. A pool is a set of servers running the same services that work together to handle client requests directed to them through a load balancer. See [Load balancing requirements for Skype for Business](#) for details

### DNS record Requirements for Server/pool roles (presumes DNS load balancing)

DEPLOYMENT SCENARIO	DNS REQUIREMENT
One Server: Persistent Chat, Director, Mediation Server, Front end server	An internal A record that resolves the fully qualified domain name (FQDN) of the server to its IP address. ServerRole.contoso.com 10.10.10.0
Pool: Persistent Chat, Director, Edge Server, Mediation Server, Front end	An internal A record that resolves the fully qualified domain name (FQDN) of each server node in the pool to its IP address. <b>Example</b> ServerRole01.contoso.com 10.10.10.1 ServerRole02.contoso.com 10.10.10.2 Multiple internal A records that resolve the fully qualified domain name (FQDN) of the pool to the IP addresses of the server nodes in the pool. <b>Example</b> ServerPool.contoso.com 10.10.10.1 ServerPool.contoso.com 10.10.10.2

### Edge Server specific DNS topics

To plan edge server deployment, review [Plan for Edge Server deployments in Skype for Business Server 2015](#), and [Advanced Edge Server DNS planning for Skype for Business Server 2015](#) which has the following sections

- [DNS disaster recovery](#)
- [DNS load balancing](#)
- [Automatic configuration without split-brain DNS](#)
- [Split-brain DNS](#)
- [Walkthrough of Skype for Business clients locating services](#)



# DNS basics

5/20/2019 • 3 minutes to read

Windows Server 2016 has built-in software that can provide DNS services, so you may want to review the available documentation such as the [DNS Policy Scenario Guide](#). You can choose a third-party solution if you prefer.

We recommend that as a best practice you dedicate a specific server in your implementation to provide DNS. You could potentially set it up on one of the servers dedicated to one of the Skype for Business server roles, but if that server was also part of a pool and got decommissioned by accident Skype for Business would malfunction until DNS services were re-established.

## DNS Records

Each mapping of a name to an IP address (and that could be an IPv4 or IPv6 address) is stored in a DNS record on the DNS server. The name is described in the DNS Report specifically as an FQDN — a Fully Qualified Domain Name. While *contoso.com* is a valid domain name, it's shorthand for *\*.contoso.com*, so it's ambiguous and could possibly refer to any server in the domain. An example of an FQDN that would refer to a single server in your domain might be **meeting01.contoso.com**.

### IMPORTANT

By default the computer name of a computer that is not joined to a domain is a host name, and not a fully qualified domain name (FQDN). Topology Builder uses FQDNs, not host names. So, you must configure a DNS suffix on the name of the computer to be deployed as an Edge Server that is not joined to a domain. **Use only standard characters** (including A-Z, a-z, 0-9, and hyphens) when assigning FQDNs to your servers running Skype for Business Server. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (that is, when the FQDN must be assigned to the SN in the certificate).

In addition to an IP address, the FQDN could map to a **VIP** — A virtual IP address. A VIP is an IP address that doesn't correspond to an actual physical network interface. A VIP often points to a pool of servers performing a server role, or to a pair of servers configured for redundancy and fault-tolerance.

There are several types of DNS record, the ones that are most relevant to this discussion are:

- **A** — an Address record or Host record, Returns a 32-bit IPv4 address. Most commonly used to map hostnames to an IP address of the host.
- **AAAA** — an IPv6 address record. Returns a 128-bit IPv6 address. Most commonly used to map hostnames to an IP address of the host.
- **CNAME** — a Canonical name record. This resolves one name to another: the DNS lookup will retry the lookup with the new name.
- **SRV** — a Service record (SRV record) specifies a service (a process on a server) that is accessed on a specific port and IP combination. The names of services requiring a service record are fixed, and can't be customized beyond making them part of your SIP domain. Some user services use Simple URLs. An SRV record must point to a location in the same SIP domain, so if you have multiple domains you'll need multiple SRV records for a given service.

## How to choose a SIP domain name

An organization's SIP domain name usually aligns with the email addresses given to its users. If a user in your organization would have an email address like Brown@contoso.com, the preferred <sip-domain> for an organization with the contoso.com domain name is simply contoso.com.

### **Multiple SIP domains**

Your organization might in some cases need several SIP domains. As an example, if Fabrikam.com was acquired by contoso.com, you might need to create a new SIP domain that Skype for Business Server recognizes and will accept connection from. When you do this, you'd need to create an additional set of all the DNS records that use contoso.com, with new FQDNs that show where to send requests for Fabrikam.

## **DNS Load Balancing**

You can use DNS to share traffic load among several servers that are set up as a server pool. To do this, you would create several A records for the pool's FQDN, each of which points to the IP address of a node in the pool.

See [DNS load balancing](#) for additional discussions of load balancing.

# DNS requirements for simple URLs in Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Review the Simple URL considerations in this topic before implementing DNS records for Skype for Business Server.

Simple URLs make joining meetings easier for your users, and make getting to Skype for Business Server administrative tools easier for administrators. Simple URLs use their own domain, which must not match any of the SIP domains you define.

Skype for Business Server supports the following three simple URLs: Meet, Dial-In, and Admin. You are required to set up simple URLs for Meet and Dial-In, and the Admin simple URL is optional. The Domain Name System (DNS) records that you need to support simple URLs depend on how you have defined these simple URLs, and whether you want to support disaster recovery for Simple URLs.

## Simple URL scope

You can configure your simple URLs to have global scope, or you can specify different simple URLs for each central site in your organization. If both a global simple URL and a site simple URL are specified, the site simple URL has precedence.

In most cases, we recommend that you set simple URLs only at the global level, so that a user's Meet simple URL does not change if they move from one site to another. The exception would be organizations that need to use different telephone numbers for dial-in users at different sites. Note that if you set one simple URL (such as the Dial-in simple URL) at a site to be a site-level simple URL, you must also set the other simple URLs at that site to be site-level as well.

You can set global simple URLs in Topology Builder. To set a simple URL at the site level, use the `Set-CsSimpleURLConfiguration` cmdlet.

Defining a simple URL will also require setting an A and/or AAAA record in your DNS configuration.

## Simple URL naming and validation rules

Topology Builder and the Skype for Business Server Management Shell cmdlets enforce several validation rules for your simple URLs. You are required to set simple URLs for Meet and Dialin, but setting one for Admin is optional. Each SIP domain must have a separate Meet simple URL, but you need only one Dialin simple URL and one Admin simple URL for your whole organization.

Each simple URL in your organization must have a unique name, and cannot be a prefix of another simple URL (for example, you could not set `SfB2015.contoso.com/Meet` as your Meet simple URL and `SfB2015.contoso.com/Meet/Dialin` as your Dialin simple URL). Simple URL names cannot contain the FQDN of any of your pools, or any port information (for example, `https://FQDN:88/meet` is not allowed). All simple URLs must start with the `https://` prefix.

Simple URLs can contain only alphanumeric characters (that is, a-z, A-Z, 0-9, and the period (.)). If you use other characters, the simple URLs might not work as expected.

## Changing Simple URLs after deployment

If you change a simple URL after initial deployment, you must be aware of how the change impacts your DNS records and certificates for simple URLs. If the base of a simple URL changes, then you must change the DNS records and certificates as well. For example, changing from <https://SfB2015.contoso.com/Meet> to <https://meet.contoso.com> changes the base URL from SfB2015.contoso.com to meet.contoso.com, so you would need to change the DNS records and certificates to refer to meet.contoso.com. If you changed the simple URL from <https://SfB2015.contoso.com/Meet> to <https://SfB2015.contoso.com/Meetings>, the base URL of SfB2015.contoso.com stays the same, so no DNS or certificate changes are needed.

Whenever you change a simple URL name, however, you must run **Enable-CsComputer** on each Director and Front End Server to register the change.

## Naming examples for Simple URLs

There are three recommended options for naming your simple URLs. Which option you choose has implications for how you set up your DNS A records and certificates which support simple URLs. In each option, you must configure one Meet simple URL for each SIP domain in your organization.

You always need just one simple URL in your whole organization for Dial-in, and one for Admin, no matter how many SIP domains you have.

In Option 1, you create a new SIP domain name for each simple URL.

If you use this option, you need a separate DNS A record for each simple URL, and each Meet simple URL must be named in your certificates.

### Simple URL Naming Option 1

SIMPLE URL	EXAMPLE
Meet	<a href="https://meet.contoso.com">https://meet.contoso.com</a> , <a href="https://meet.fabrikam.com">https://meet.fabrikam.com</a> , and so on (one for each SIP domain in your organization)
Dial-in	<a href="https://dialin.contoso.com">https://dialin.contoso.com</a>
Admin	<a href="https://admin.contoso.com">https://admin.contoso.com</a>

With Option 2, simple URLs are based on the domain name SfB2015.contoso.com. Therefore, you need only one DNS A record which enables all three types of simple URLs. This DNS A record references SfB2015.contoso.com. Additionally, you still need separate DNS A records for other SIP domains in your organization.

### Simple URL Naming Option 2

SIMPLE URL	EXAMPLE
Meet	<a href="https://SfB2015.contoso.com/Meet">https://SfB2015.contoso.com/Meet</a> , <a href="https://SfB2015.fabrikam.com/Meet">https://SfB2015.fabrikam.com/Meet</a> , and so on (one for each SIP domain in your organization)
Dial-in	<a href="https://SfB2015.contoso.com/Dialin">https://SfB2015.contoso.com/Dialin</a>
Admin	<a href="https://SfB2015.contoso.com/Admin">https://SfB2015.contoso.com/Admin</a>

Option 3 is most useful if you have many SIP domains, and you want them to have separate Meet simple URLs but want to minimize the DNS record and certificate requirements for these simple URLs.

### Simple URL Naming Option 3

SIMPLE URL	EXAMPLE
Meet	<a href="https://SfB2015.contoso.com/contosoSIPdomain/Meet">https://SfB2015.contoso.com/contosoSIPdomain/Meet</a> <a href="https://SfB2015.contoso.com/fabrikamSIPdomain/Meet">https://SfB2015.contoso.com/fabrikamSIPdomain/Meet</a>
Dial-in	<a href="https://SfB2015.contoso.com/Dialin">https://SfB2015.contoso.com/Dialin</a>
Admin	<a href="https://SfB2015.contoso.com/Admin">https://SfB2015.contoso.com/Admin</a>

## Disaster Recovery option for simple URLs

If you have multiple sites that contain Front End pools and your DNS provider supports GeoDNS, you can set up your DNS records for Simple URLs to support disaster recovery, so that Simple URL functionality continues even if one entire Front End pool goes down. This disaster recovery feature supports the Meet and Dial-In simple URLs.

To configure this, create two GeoDNS addresses. Each address has two DNS A or CNAME records that resolve to two pools which are paired together for disaster recovery purposes. One GeoDNS address is used for internal access, and resolves to the internal web FQDN or load balancer IP address for the two pools. The other GeoDNS address is used for external access and resolves to the external web FQDN or load balancer IP address for the two pools. The following is an example for the Meet simple URL, using the FQDNs for the pools.

```
Meet-int.geolb.contoso.com
  Pool1InternalWebFQDN.contoso.com
  Pool2InternalWebFQDN.contoso.com
```

```
Meet-ext.geolb.contoso.com
  Pool1ExternalWebFQDN.contoso.com
  Pool2ExternalWebFQDN.contoso.com
```

Then create CNAME records that resolve your Meet simple URL (such as `meet.contoso.com`) to the two GeoDNS addresses.

### NOTE

If your network uses hairpinning (routing all your Simple URL traffic through the external link, including traffic that comes from within your organization), then you can just configure the external GeoDNS address and resolve your Meet simple URL to only that external address.

When you use this method, you can configure each GeoDNS address to use either a round robin method to distribute requests to the two pools, or to connect primarily to one pool (such as the pool located geographically closer) and use the other pool only in case of connectivity failure.

You can set up the same configuration for the Dial-In simple URL. To do so, create additional records like those in the previous example, substituting `dialin` for `meet` in the DNS records. For the Admin simple URL, use one of the three options listed earlier in this section.

Once this configuration is set up, you must use a monitoring application to set up HTTP monitoring to watch for failures. For external access, monitor to make sure that HTTPS GET `lyncdiscover.` requests to the external web FQDN or load balancer IP address for the two pools are successful. For example, the following requests must not contain any **ACCEPT** header and must return **200 OK**.

```
HTTPS GET Pool1ExternalWebFQDN.contoso.com/autodiscover/autodiscover/service.svc/root
HTTPS GET Pool2ExternalWebFQDN.contoso.com/autodiscover/autodiscover/service.svc/root
```

For internal access, you must monitor port 5061 on the internal web FQDN or load balancer IP address for the two pools. If any connectivity failures are detected, the VIP for these pools must close ports 80, 443 and 4443.

# Advanced Edge Server DNS planning for Skype for Business Server

7/17/2019 • 12 minutes to read

**Summary:** Review scenarios for Skype for Business Server deployment options. Whether you want a single server or prefer a server pool with DNS or HLB, this topic should help.

When it comes to Domain Name System (DNS) planning for Skype for Business Server, there are a lot of factors that may play into your decision. If your organization's domain structure's already in place, this may be a matter of reviewing how you're going to proceed. We'll begin with the topics found below:

- [Walkthrough of Skype for Business clients locating services](#)
- [Split-brain DNS](#)
- [Automatic configuration without split-brain DNS](#)
- [DNS disaster recovery](#)
- [DNS load balancing](#)

## Walkthrough of Skype for Business clients locating services

Skype for Business clients are similar to previous versions of Lync clients in how they find and access services in Skype for Business Server. This section details the server location process.

1. `lyncdiscoverinternal.<domain>`

*This is an A host record for the Autodiscover service on the internal web services.*

2. `lyncdiscover.<domain>`

*This is an A host record for the Autodiscover service on the external web services.*

3. `_sipinternaltls._tcp.<domain>`

*This is a SRV record for internal TLS connections.*

4. `_sip._tls.<domain>`

*This is a SRV record for external TLS connections.*

5. `sipinternal.<domain>`

*This is an A host record for the Front End pool or Director, resolvable only on the internal network.*

6. `sip.<domain>`

*This is an A host record for the Front End pool or Director, resolvable only on the internal network.*

7. `sipexternal.<domain>`

*This is an A host record for the Access Edge service, when the client is external.*

The Autodiscover service is always favored as that's the preferred method for service location, and the others are fallback methods.

## NOTE

When you're creating SRV records, it's important to remember that they need to point to a DNS A (and AAAA if you're using IPv6 addressing) in the same domain in which the DNS SRV record's being created. For example, if they SRV record's in contoso.com, the A (and AAAA) record it points to can't be in fabrikam.com.

If you're inclined to do it, you can set your mobile device up for manual discovery of services. If that's what you're looking to do, each user needs to configure their mobile device settings with the full internal and external Autodiscover service URIs, including the protocol and path, as follows:

- For external access: `https://<ExtPoolFQDN>/Autodiscover/autodiscover.service.svc/Root`
- For internal access: `https://<IntPoolFQDN>/AutoDiscover/AutoDiscover.svc/Root`

We do recommend you use automatic discovery as opposed to manual discovery. But if you're doing some troubleshooting or testing, manual settings can be very helpful.

## Split-brain DNS

This is a DNS configuration where you have two DNS zones with the same namespace. The first DNS zone handles internal requests, while the second DNS zone handles external requests.

Why would a company do this? They may have a requirement to use the same namespace internally and externally, but of course this will lead to many DNS SRV and A records being unique to one zone or another, and where there is duplication, the IP addresses associated with these records would be unique.

This presents some challenges. The most important is that split-brain DNS is **not supported** for Mobility. This is because of the LyncDiscover and LyncDiscoverInternal DNS records (LyncDiscover has to be defined on your external DNS server, while LyncDiscoverInternal has to be defined on your internal DNS server).

We'll list the DNS records for the internal and external zones here, but you can find detailed examples on the Edge Server environmental requirements section.

### Internal DNS

- Contains a DNS zone called (for example) contoso.com, for which it's authoritative.
- This internal contoso.com contains:
  - DNS A and AAAA (if you're using IPv6 addressing) records for your Front End pool, Director pool or Director pool name, and all internal servers running Skype for Business Server in your organization's network.
  - DNS A and AAAA (if you're using IPv6 addressing) records for your Edge internal interface for each Skype for Business Server Edge Server in your perimeter network.
  - DNS A and AAAA (if you're using IPv6 addressing) records for the internal interface of each reverse proxy server in your perimeter network (which is **optional** for management of a reverse proxy).
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for internal Skype for Business Server client autoconfiguration (which is **optional**).
  - DNS A and AAAA (if you're using IPv6 addressing) or CNAME records for automatic discovery of Skype for Business Server Web Services (which is **optional**).
- All your Skype for Business Server internal Edge interfaces in your perimeter network use this internal DNS zone for resolving queries to contoso.com.
- All servers running Skype for Business Server, and clients running Skype for Business Server in the



corporate network, point to internal DNS servers for resolving queries to contoso.com, or they use the Host file on each Edge Server and list A and AAAA (if you're using IPv6 addressing) records for the next hop server (specifically for the Director or Director pool VIP, Front End pool VIP, or Standard Edition server).

## External DNS

- Contains a DNS zone called (for example) contoso.com, for which it's authoritative.
- This external contoso.com contains:
  - DNS A and AAAA (if you're using IPv6 addressing), or CNAME records, for automatic discovery of Skype for Business Server web services. This is for use with mobility.
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for the Edge external interface of each Skype for Business Server Edge Server or hardware load balanced (HLB) VIP in the perimeter network.
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for the external interface of the Reverse proxy server or (VIP for a pool of Reverse proxy servers), in the perimeter network.
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for Skype for Business Server client autoconfiguration (**optional**).

## Automatic configuration without split-brain DNS

If you don't use split-brain DNS, internal automatic configuration of clients running Skype for Business won't work unless you're using one of the workarounds we have here. Why not? Because Skype for Business Server requires the user's SIP URI to match the domain of the Front End pool designated for automatic configuration. This hasn't changed from earlier versions of Lync Server.

So, if you have two SIP domains in use, you'd need these DNS SRV records:

- `_sipinternaltls._tcp.contoso.com. 86400 IN SRV 0 0 5061 pool01.contoso.com`

*If a user signs in as bob@contoso.com, this record would work for automatic configuration, as the user's SIP domain matches the domain of the Front End pool (contoso.com).*

- `_sipinternaltls._tcp.fabrikam.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com`

*If a user signs in as alice@fabrikam.com, this record would work for automatic configuration of the second domain, again because the SIP domain matches the Front End pool for that domain.*

To take the example further, this would not work:

- `_sipinternaltls._tcp.litwareinc.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com`

*A user signing in as tim@litwareinc.com won't work for automatic configuration, because his SIP domain (litwareinc.com) doesn't match the domain in the pool (fabrikam.com).*

So now that we know all that, if you need automatic requirement for your Skype for Business clients without split-brain DNS, you have these options:

- **Group Policy Objects**

You can use Group Policy Objects (GPOs) to populate the correct server values.

### NOTE

This option doesn't enable automatic configuration, but it does automate manual configuration. If this approach is used, the SRV records associated with automatic configuration aren't required.

- **Matching internal zone**

You'll need to create a zone in your internal DNS that matches your external DNS zone (for example, contoso.com), and then create DNS A (and AAAA if you're using IPv6 addressing) records that correspond to the Skype for Business Server pool used for automatic configuration.

For example, if you have a user homed on pool01.contoso.net, but signs into Skype for Business as bob@contoso.com, create an internal DNS zone called contoso.com, and inside it you need to create a DNS A (and AAAA if IPv6 addressing's being used) record for pool01.contoso.com.

- **Pin-point internal zone**

If creating an entire zone in your internal DNS isn't an option for you, you can create pin-point (dedicated) zones that correspond to the SRV records required for automatic configuration, and populate those zones using dnscmd.exe. Dnscmd.exe is required because the DNS user interface won't support the creation of pin-point zones.

For example, if your SIP domain is contoso.com, and you have a Front End pool called pool01 that contains two Front End Servers, you'll need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.contoso.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.contoso.com. @ SRV 0 0 5061 pool01.contoso.com.
dnscmd . /zoneadd pool01.contoso.com. /dsprimary
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
```

You may have a second SIP domain in your environment. In that case, you'll need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.fabrikam.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.fabrikam.com. @ SRV 0 0 5061 pool01.fabrikam.com.
dnscmd . /zoneadd pool01.fabrikam.com. /dsprimary
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.fabrikam.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.fabrikam.com. @ AAAA <IPv6 address>
```

**NOTE**

You'll see the Front End pool FQDN appears twice, but with two different IP addresses. That's because DNS load balancing is used. If HLB is used, there'd only be a single Front End pool entry.

**NOTE**

Also, the Front End pool FQDN values change between the contoso.com and fabrikam.com examples, but the IP addresses remain the same. That's because users who're signing in from either SIP domain will be using the same Front End pool for automatic configuration.

## DNS disaster recovery

To configure DNS to redirect Skype for Business Server web traffic to your disaster recover (DR) and failover sites, you need to use a DNS provider that supports GeoDNS. You can set up your DNS records to support disaster recover, so that features that use web services continue even if one entire Front End pool goes down. This DR

feature supports the Autodiscover, Meet and Dial-in simple URLs.

You define and configure additional DNS host A (AAAA if using IPv6) records for internal and external resolution of web services at your GeoDNS provider. The following details assume paired pools, geographically dispersed, and that the GeoDNS supported by your provider **either** has round-robin DNS **or** is configured to use Pool1 as primary and fails over to Pool2 in the event of any communications loss or power failure.

All the DNS records in this table are examples.

GEODNS RECORD	POOL RECORDS	CNAME RECORDS	DNS SETTINGS (SELECT ONE OPTION)
Meet-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1InternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Meet-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Dialin-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1InternalWebFQDN.contoso.com Dialin.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Dialin-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Dialin.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Lyncdiscoverint-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Lyncdiscoverinternal.contoso.com alias to Pool1InternalWebFQDN.contoso.com Lyncdiscoverinternal.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Lyncdiscover-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Lyncdiscover.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Lyncdiscover.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure

GEODNS RECORD	POOL RECORDS	CNAME RECORDS	DNS SETTINGS (SELECT ONE OPTION)
Scheduler-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1InternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Scheduler-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure

## DNS load balancing

DNS load balancing is usually implemented at the application level. The application (for example, a client running Skype for Business), tries to connect to a server in a pool by connecting to one of the IP addresses returned from the DNS A and AAAA (if IPv6 addressing is used) record query for the pool FQDN.

For example, if there are three Front End Servers in a pool named pool01.contoso.com, the following would happen:

- Clients running Skype for Business query DNS for pool01.contoso.com. The query returns three IP addresses and caches them as follows (in some order):

pool01.contoso.com	192.168.10.90
pool01.contoso.com	192.168.10.91
pool01.contoso.com	192.168.10.92

- The client tries to establish a TCP connection to one of the IP addresses. If that fails, it'll try the next IP address it's cached from that list.
- If the TCP connection succeeds, the client negotiates TLS to connect to the primary registrar on pool01.contoso.com.
- If the client tries all cached entries without a successful connection, the user receives a notification that no servers running Skype for Business Server are available at the moment.

### NOTE

DNS-based load balancing is different from DNS round robin (DNS RR), which typically refers to load balancing by relying on DNS to give a different order of IP addresses for the servers in your pool. Typically, DNS RR enables load distribution, but it won't allow you to enable failover. For example, if the connection to the one IP address returned by your DNS A (or AAAA in an IPv6 scenario) query fails, that connection will fail. That makes DNS RR less reliable than DNS-based load balancing. You can still use DNS RR in conjunction with DNS-based load balancing if you need to do that.

You use DNS load balancing to:

- Load balance server-to-server SIP to the Edge Servers.
- Load balance Unified Communication Application Services (UCAS) applications, such as Conferencing Auto Attendant, Response Group, and Call Park.
- Prevent new connections to UCAS applications (also known as draining).
- Load balance all client-to-server traffic between clients and Edge Servers.

You can't use DNS load balancing for:

- Client-to-server web traffic to your Front End Servers or a Director.

To go a little more in-depth on how a DNS SRV record's selected when multiple DNS records are returned by a query, the Access Edge service always picks the record with the lowest numeric priority and, if a tie-breaker is needed, the highest numeric weight. This is consistent with [Internet Engineering Task Force documentation](#).

So, for example, if your first DNS SRV record has a weight of 20 and a priority of 40, and your second DNS SRV record has a weight of 10 and a priority of 50, the first record's going to be chosen because it has the lower priority of 40. Priority always goes first, and that's the host that a client will target first. What if there are two targets with the same priority?

In that case, weight comes into consideration. Larger weights should be given a high probability, in this circumstance, of being selected. DNS administrators should use weight 0 when there isn't any server selection to do. In the presence of records containing weights greater than 0, records with weight 0 have a very small chance of being selected.

So, then, what happens if multiple DNS SRV records with equal priority and weight are returned? In this situation the Access Edge service will choose the SRV record that it got from the DNS server first.

# Port and protocol requirements for servers

5/20/2019 • 13 minutes to read

**Summary:** Review the port usage considerations before implementing Skype for Business Server.

Skype for Business Server requires that specific ports on the external and internal firewalls be open. Additionally, if Internet Protocol security (IPsec) is deployed in your organization, IPsec must be disabled over the range of ports used for the delivery of audio, video, and panorama video.

While this may seem a bit daunting at first, the heavy lifting for planning this can be done using the [Skype for Business Server 2015 Planning Tool](#). Once you've gone through the wizard's questions about what features you plan to use, for each site you define you can view the Firewall Report within the Edge Admin Report, and use the information listed there to create your firewall rules. You can also make adjustments to many of the names and IP addresses used, for details see [Review the Firewall Report](#). Keep in mind you can export the Edge Admin Report to an Excel spreadsheet, and the Firewall Report will be one of the worksheets in the file.

You can also find the information in these tables in diagram form by reviewing the Protocol Workloads poster linked off of the [Technical diagrams for Skype for Business Server 2015](#) article.

## NOTE

- If you're implementing Skype for Business Online (O365) refer to [Office 365 URLs and IP address ranges](#). Hybrid environments will need to reference this topic and also [Plan hybrid connectivity](#).
- You can have hardware or software firewalls, we don't require specific models or versions. What matters is what ports are whitelisted so the firewall won't impair the functioning of Skype for Business Server.

## Port and Protocol Details

This section summarizes the ports and protocols used by servers, load balancers, and clients in a Skype for Business Server deployment.

## NOTE

When Skype for Business Server starts, it opens the required ports in the Windows Firewall. Windows Firewall should already be running in most normal applications, but if it is not being used Skype for Business Server will function without it.

For details about firewall configuration for edge components, see [Edge Server scenarios in Skype for Business Server 2015](#).

The following table lists the ports that need to be open on each internal server role.

### Required Server Ports (by Server Role)

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
All Servers	SQL Browser	1434	UDP	SQL Browser for the local replicated copy of the Central Management Store database.

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
Front End Servers	Skype for Business Server Front-End service	5060	TCP	Optionally used by Standard Edition servers and Front End Servers for static routes to trusted services, such as remote call control servers.
Front End Servers	Skype for Business Server Front-End service	5061	TCP (TLS)	Used by Standard Edition servers and Front End pools for all internal SIP communications between servers (MTLS), for SIP communications between Server and Client (TLS) and for SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with a Monitoring Server.
Front End Servers	Skype for Business Server Front-End service	444	HTTPS TCP	Used for HTTPS communication between the Focus (the Skype for Business Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Survivable Branch Appliances and Front End Servers.
Front End Servers	Skype for Business Server Front-End service	135	DCOM and remote procedure call (RPC)	Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization.
Front End Servers	Skype for Business Server IM Conferencing service	5062	TCP	Used for incoming SIP requests for instant messaging (IM) conferencing.

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
Front End Servers	Skype for Business Server Web Conferencing service	8057	TCP (TLS)	Used to listen for Persistent Shared Object Model (PSOM) connections from client.
Front End Servers	Skype for Business Server Web Conferencing Compatibility service	8058	TCP (TLS)	Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Skype for Business Server.
Front End Servers	Skype for Business Server Audio/Video Conferencing service	5063	TCP	Used for incoming SIP requests for audio/video (A/V) conferencing.
Front End Servers	Skype for Business Server Audio/Video Conferencing service	57501-65535	TCP/UDP	Media port range used for video conferencing.
Front End Servers	Skype for Business Server Web Compatibility service	80	HTTP	Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components) when HTTPS is not used.
Front End Servers	Skype for Business Server Web Compatibility service	443	HTTPS	Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components).
Front End Servers	Skype for Business Server Web Compatibility service	8080	TCP and HTTP	Used by web components for external access.
Front End Servers	Web server component	4443	HTTPS	HTTPS (from Reverse Proxy) and HTTPS Front End inter-pool communications for Autodiscover sign-in.
Front End Servers	Web server component	8060	TCP (MTLS)	
Front End Servers	Web server component	8061	TCP (MTLS)	



SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
Front End Servers	Mobility Services component	5086	TCP (MTLS)	SIP port used by Mobility Services internal processes
Front End Servers	Mobility Services component	5087	TCP (MTLS)	SIP port used by Mobility Services internal processes
Front End Servers	Mobility Services component	443	HTTPS	
Front End Servers	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	5064	TCP	Used for incoming SIP requests for dial-in conferencing.
Front End Servers	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	5072	TCP	Used for incoming SIP requests for Attendant (dial in conferencing).
Front End Servers that also run a Collocated Mediation Server	Skype for Business Server Mediation service	5070	TCP	Used by the Mediation Server for incoming requests from the Front End Server to the Mediation Server.
Front End Servers that also run a Collocated Mediation Server	Skype for Business Server Mediation service	5067	TCP (TLS)	Used for incoming SIP requests from the PSTN gateway to the Mediation Server.
Front End Servers that also run a Collocated Mediation Server	Skype for Business Server Mediation service	5068	TCP	Used for incoming SIP requests from the PSTN gateway to the Mediation Server.
Front End Servers that also run a Collocated Mediation Server	Skype for Business Server Mediation service	5081	TCP	Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.
Front End Servers that also run a Collocated Mediation Server	Skype for Business Server Mediation service	5082	TCP (TLS)	Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.
Front End Servers	Skype for Business Server Application Sharing service	5065	TCP	Used for incoming SIP listening requests for application sharing.
Front End Servers	Skype for Business Server Application Sharing service	49152-65535	TCP	Media port range used for application sharing.

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
Front End Servers	Skype for Business Server Conferencing Announcement service	5073	TCP	Used for incoming SIP requests for the Skype for Business Server Conferencing Announcement service (that is, for dial-in conferencing).
Front End Servers	Skype for Business Server Call Park service	5075	TCP	Used for incoming SIP requests for the Call Park application.
Front End Servers	Skype for Business Server Audio Test service	5076	TCP	Used for incoming SIP requests for the Audio Test service.
Front End Servers	Not applicable	5066	TCP	Used for outbound Enhanced 9-1-1 (E9-1-1) gateway.
Front End Servers	Skype for Business Server Response Group service	5071	TCP	Used for incoming SIP requests for the Response Group application.
Front End Servers	Skype for Business Server Response Group service	8404	TCP (MTLS)	Used for incoming SIP requests for the Response Group application.
Front End Servers	Skype for Business Server Bandwidth Policy Service	5080	TCP	Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic.
Front End Servers	Skype for Business Server File Share server access	445	SMB/TCP	Used to retrieve Address book, meeting content, and other items stored on the File Share server.
Front End Servers	Skype for Business Server Bandwidth Policy Service	448	TCP	Used for call admission control by the Skype for Business Server Bandwidth Policy Service.
Front End Servers where the Central Management store resides	Skype for Business Server Master Replicator Agent service	445	TCP	Used to push configuration data from the Central Management store to servers running Skype for Business Server.

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
All Servers	SQL Browser	1434	UDP	SQL Browser for local replicated copy of Central Management store data in local SQL Server instance
All internal servers	Various	49152-57500	TCP/UDP	Media port range used for audio conferencing on all internal servers. Used by all servers that terminate audio: Front End Servers (for Skype for Business Server Conferencing Attendant service, Skype for Business Server Conferencing Announcement service, and Skype for Business Server Audio/Video Conferencing service), and Mediation Server.
Office Web Apps Servers		443		Used by Skype for Business Server to connect to Office Web Apps Server.
Directors	Skype for Business Server Front-End service	5060	TCP	Optionally used for static routes to trusted services, such as remote call control servers.
Directors	Skype for Business Server Front-End service	444	HTTPS TCP	Inter-server communication between Front End and Director. Additionally, client certificate publish (to Front End Servers) or validate if the client certificate has already been published.
Directors	Skype for Business Server Web Compatibility service	80	TCP	Used for initial communication from Directors to the web farm FQDNs (the URLs used by IIS web components). In normal operation, will switch to HTTPS traffic, using port 443 and protocol type TCP.

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
Directors	Skype for Business Server Web Compatibility service	443	HTTPS	Used for communication from Directors to the web farm FQDNs (the URLs used by IIS web components).
Directors	Skype for Business Server Front-End service	5061	TCP	Used for internal communications between servers and for client connections.
Mediation Servers	Skype for Business Server Mediation service	5070	TCP	Used by the Mediation Server for incoming requests from the Front End Server.
Mediation Servers	Skype for Business Server Mediation service	5067	TCP (TLS)	Used for incoming SIP requests from the PSTN gateway.
Mediation Servers	Skype for Business Server Mediation service	5068	TCP	Used for incoming SIP requests from the PSTN gateway.
Mediation Servers	Skype for Business Server Mediation service	5070	TCP (MTLS)	Used for SIP requests from the Front End Servers.
Persistent Chat Front End Server	Persistent Chat SIP	5041	TCP (MTLS)	
Persistent Chat Front End Server	Persistent Chat Windows Communication Foundation (WCF)	881	TCP (TLS) and TCP (MTLS)	
Persistent Chat Front End Server	Persistent Chat File Transfer Service	443	TCP (TLS)	

#### NOTE

Some remote call control scenarios require a TCP connection between the Front End Server or Director and the PBX. Although Skype for Business Server no longer uses TCP port 5060, during remote call control deployment you create a trusted server configuration, which associates the RCC Line Server FQDN with the TCP port that the Front End Server or Director will use to connect to the PBX system. For details, see the **CsTrustedApplicationComputer** cmdlet in the Skype for Business Server Management Shell documentation.

For your pools that use only hardware load balancing (not DNS load balancing), the following table shows the ports that need to open the hardware load balancers.

#### Hardware Load Balancer Ports if Using Only Hardware Load Balancing

LOAD BALANCER	PORT	PROTOCOL
Front End Server load balancer	5061	TCP (TLS)
Front End Server load balancer	444	HTTPS
Front End Server load balancer	135	DCOM and remote procedure call (RPC)
Front End Server load balancer	80	HTTP
Front End Server load balancer	8080	TCP - Client and device retrieval of root certificate from Front End Server - clients and devices authenticated by NTLM
Front End Server load balancer	443	HTTPS
Front End Server load balancer	4443	HTTPS (from reverse proxy)
Front End Server load balancer	5072	TCP
Front End Server load balancer	5073	TCP
Front End Server load balancer	5075	TCP
Front End Server load balancer	5076	TCP
Front End Server load balancer	5071	TCP
Front End Server load balancer	5080	TCP
Front End Server load balancer	448	TCP
Mediation Server load balancer	5070	TCP
Front End Server load balancer (if the pool also runs Mediation Server)	5070	TCP
Director load balancer	443	HTTPS
Director load balancer	444	HTTPS
Director load balancer	5061	TCP
Director load balancer	4443	HTTPS (from reverse proxy)

Your Front End pools and Director pools that use DNS load balancing also must have a hardware load balancer deployed. The following table shows the ports that need to be open on these hardware load balancers.

### Hardware Load Balancer Ports if Using DNS Load Balancing

LOAD BALANCER	PORT	PROTOCOL
Front End Server load balancer	80	HTTP
Front End Server load balancer	443	HTTPS
Front End Server load balancer	8080	TCP - Client and device retrieval of root certificate from Front End Server - clients and devices authenticated by NTLM
Front End Server load balancer	4443	HTTPS (from reverse proxy)
Director load balancer	443	HTTPS
Director load balancer	4443	HTTPS (from reverse proxy)

### Required Client Ports

COMPONENT	PORT	PROTOCOL	NOTES
Clients	67/68	DHCP	Used by Skype for Business Server to find the Registrar FQDN (that is, if DNS SRV fails and manual settings are not configured).
Clients	443	TCP (TLS)	Used for client-to-server SIP traffic for external user access.
Clients	443	TCP (PSOM/TLS)	Used for external user access to web conferencing sessions.
Clients	443	TCP (STUN/MSTURN)	Used for external user access to A/V sessions and media (TCP)
Clients	3478	UDP (STUN/MSTURN)	Used for external user access to A/V sessions and media (UDP)
Clients	5061	TCP (MTLS)	Used for client-to-server SIP traffic for external user access.
Clients	6891-6901	TCP	Used for file transfer between Skype for Business clients and previous clients.
Clients	1024-65535 *	TCP/UDP	Audio port range (minimum of 20 ports required)
Clients	1024-65535 *	TCP/UDP	Video port range (minimum of 20 ports required).

COMPONENT	PORT	PROTOCOL	NOTES
Clients	1024-65535 *	TCP	Peer-to-peer file transfer (for conferencing file transfer, clients use PSOM).
Clients	1024-65535 *	TCP	Application sharing.
Aastra 6721ip common area phone Aastra 6725ip desk phone HP 4110 IP Phone (common area phone) HP 4120 IP Phone (desk phone) Polycom CX500 IP common area phone Polycom CX600 IP desk phone Polycom CX700 IP desk phone Polycom CX3000 IP conference phone	67/68	DHCP	Used by the listed devices to find the Skype for Business Server certificate, provisioning FQDN, and Registrar FQDN.

\* To configure specific ports for these media types, use the CsConferencingConfiguration cmdlet (ClientMediaPortRangeEnabled, ClientMediaPort, and ClientMediaPortRange parameters).

#### NOTE

The setup programs for Skype for Business clients automatically create the required operating-system firewall exceptions on the client computer.

#### NOTE

The ports that are used for external user access are required for any scenario in which the client must traverse the organization's firewall (for example, any external communications or meetings hosted by other organizations).

## IPsec exceptions

For enterprise networks where Internet Protocol security (IPsec) (see IETF RFC 4301-4309) has been deployed, IPsec must be disabled over the range of ports used for the delivery of audio, video, and panoramic video. The recommendation is motivated by the need to avoid any delay in the allocation of media ports due to IPsec negotiation.

The following table explains the recommended IPsec exception settings.

### Recommended IPsec Exceptions

RULE NAME	SOURCE IP	DESTINATION IP	PROTOCOL	SOURCE PORT	DESTINATION PORT	AUTHENTICATION REQUIREMENT
A/V Edge Server Internal Inbound	Any	A/V Edge Server Internal	UDP and TCP	Any	Any	Do not authenticate

<b>RULE NAME</b>	<b>SOURCE IP</b>	<b>DESTINATION IP</b>	<b>PROTOCOL</b>	<b>SOURCE PORT</b>	<b>DESTINATION PORT</b>	<b>AUTHENTICATI ON REQUIREMENT</b>
A/V Edge Server External Inbound	Any	A/V Edge Server External	UDP and TCP	Any	Any	Do not authenticate
A/V Edge Server Internal Outbound	A/V Edge Server Internal	Any	UDP & TCP	Any	Any	Do not authenticate
A/V Edge Server External Outbound	A/V Edge Server External	Any	UDP and TCP	Any	Any	Do not authenticate
Mediation Server Inbound	Any	Mediation Server(s)	UDP and TCP	Any	Any	Do not authenticate
Mediation Server Outbound	Mediation Server(s)	Any	UDP and TCP	Any	Any	Do not authenticate
Conferencing Attendant Inbound	Any	Front End Server running Conferencing Attendant	UDP and TCP	Any	Any	Do not authenticate
Conferencing Attendant Outbound	Front End Server running Conferencing Attendant	Any	UDP and TCP	Any	Any	Do not authenticate
A/V Conferencing Inbound	Any	Front End Servers	UDP and TCP	Any	Any	Do not authenticate
A/V Conferencing Outbound	Front End Servers	Any	UDP and TCP	Any	Any	Do not authenticate
Exchange Inbound	Any	Exchange Unified Messaging	UDP and TCP	Any	Any	Do not authenticate
Application Sharing Servers Inbound	Any	Application Sharing Servers	TCP	Any	Any	Do not authenticate
Application Sharing Server Outbound	Application Sharing Servers	Any	TCP	Any	Any	Do not authenticate



<b>RULE NAME</b>	<b>SOURCE IP</b>	<b>DESTINATION IP</b>	<b>PROTOCOL</b>	<b>SOURCE PORT</b>	<b>DESTINATION PORT</b>	<b>AUTHENTICATI ON REQUIREMENT</b>
Exchange Outbound	Exchange Unified Messaging	Any	UDP and TCP	Any	Any	Do not authenticate
Clients	Any	Any	UDP	Specified media port range	Any	Do not authenticate

# Discussing Authentication and Authorization in Skype for Business

5/20/2019 • 2 minutes to read

Authentication and authorization are related concepts, but do different work for you (though both are necessary). Put in simple terms, authentication (AuthN) depends on secrets only a valid user knows or has, and that can be a password, code, fingerprint, certificate, a combination of claims about the user that are true, or a combination of these things used together. AuthN is a process out to prove you are who you say you are.

Authorization (AuthZ) is concerned with what you have access to after you've proven who you are. It determines what you've been allowed to see, edit, and otherwise access. For example, you may have powerful Site Collection Administrator access to SharePoint Online, but if you switch to another online workload, like Skype for Business Online, you may have the privileges to troubleshoot user issues, not change the configuration of the server or servers. In a third workload, such as Exchange Online, you might only have the average user's access. AuthZ checks what and how much access you have to services/workloads, applications, files, and other data.

Our examples involve online properties like SharePoint and Exchange online, but the processes of AuthN and AuthZ work on-premises and in a hybrid premises the same way. Ultimately, tools like AAD Connect and ADFS become involved in the AuthN and AuthZ story by either synchronizing on-premises accounts and passwords into the Cloud's AD (which is Azure AD in the case of either Office 365 or Azure), or intruding in the flow of AuthZ so that a user isn't frequently prompted for their credentials, say when switching between workloads in the Cloud, creating Single Sign-On scenarios. But they aren't, in themselves, responsible AuthN or AuthZ, just part of the mechanics.

Today, many technologies consider these processes (AuthN and AuthZ) to be one mechanism, and you'll hear many references to authentication process that also include authorization in them. It's important to remember that the first step in user access is AuthN, proving you are who you say you are, and that AuthZ uses the knowledge of who the user is to determine what he or she has access to (as you'll see with Open Authorization or OAuth).

## Authentication and Authorization Planning Topics

[How to use Modern Authentication \(ADAL\) with Skype for Business](#)

[Skype for Business topologies supported with Modern Authentication](#)

[Planning to turn off Legacy authentication methods internally and externally to your network.](#)

# Skype for Business topologies supported with Modern Authentication

5/23/2019 • 4 minutes to read

This article lists what online and on-premises topologies are supported with Modern Authentication in Skype for Business, as well as security features that apply to each topology.

## Modern Authentication in Skype for Business

Skype for Business can leverage security advantages of Modern Authentication. Because Skype for Business works closely with Exchange, the login behaviour Skype for Business client users will see will also be effected by the MA status of Exchange. This will also apply if you have a Skype for Business split-domain hybrid. That's a lot of moving parts, but the aim here is an easy to visualize list of supported topologies.

Given Skype for Business, Skype for Business online, Exchange Server, and Exchange online, what topologies are supported with MA?

### Supported MA topologies in Skype for Business

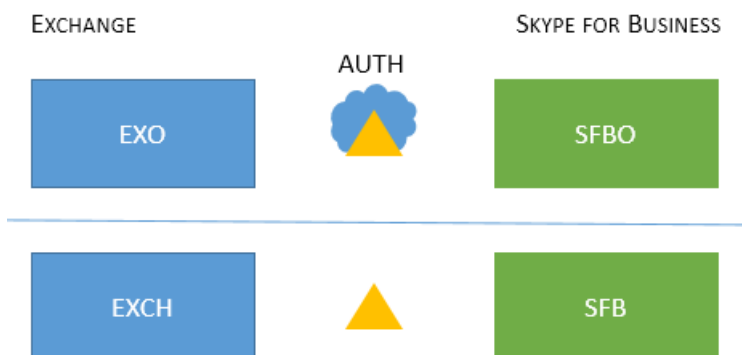
There are potentially two server applications, and two Office 365 workloads, involved with Skype for Business topologies used by MA.

- Skype for Business server (CU 5) on-premises
- Skype for Business online (SFBO)
- Exchange server on-premises
- Exchange server online (EXO)

Another important part of MA is knowing where the authentication (authN) and authorization (authZ) of users will take place. The two options are:

- Azure AD, online in the Microsoft Cloud
- Active Directory Federation Server (ADFS) on-premises

So it looks a bit like this, with EXO and SFBO in the Cloud with Azure AD, and Exchange Server (EXCH) and Skype for Business server (SFB) on-prem.



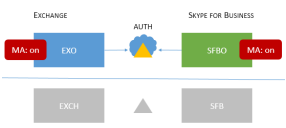
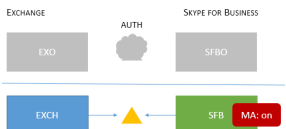
Here are the supported topologies. Please note the key for the graphics:

- If the icon is dimmed or grey, it is not used in the scenario.

- EXO is Exchange Online.
- SFBO is Skype for Business Online.
- EXCH is Exchange on-premises.
- SFB is Skype for Business on-premises.
- Authorizing servers are represented by triangles, for example, the Azure AD is a triangle with a cloud behind it.
- Arrows point at the authorizing server that will be used when clients try to reach the specified server resource.

First, let's cover MA with Skype for Business in both On-premises-only or Cloud-only topologies.

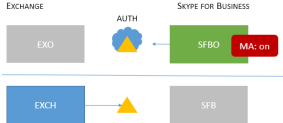


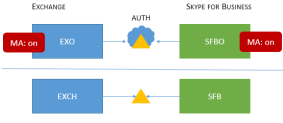
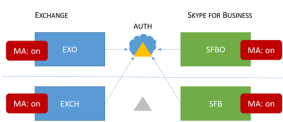
**IMPORTANT**  
 Are you ready to set up Modern Authentication in Skype for Business Online? The steps to enable this feature are right [here](#).

TOPOLOGY NAME	EXAMPLE	DESCRIPTION	SUPPORTED
Cloud only	 <p>Users homed/mailboxes located: Online</p>	<p>MA is on for both EXO and SFBO.          Therefore, the authorization server is Azure AD.</p>	<p>Multi-factor authentication (MFA), Client-certificate based authentication (CBA), Conditional Access (CA)/Mobile Application Management (MAM) with Intune. *</p>
On-prem only	 <p>Users homed/mailboxes located: On-premises</p>	<p>MA is on for SFB on-premises.          Therefore, the authorization server is ADFS.          For configuration details, please see <a href="#">this article</a>.</p>	<p>MFA (Windows Desktop only - mobile clients are not supported). No Exchange integration features.  <b>We do not recommend this approach. Please see here:</b>  <a href="https://aka.ms/ModernAuthOverview">https://aka.ms/ModernAuthOverview</a></p>

**IMPORTANT**  
 It's recommended that the MA state be the same across Skype for Business and Exchange (and their online counterparts) to reduce the number of prompts.

Mixed topologies involve combinations of SFB split-domain hybrids. These are the Mixed topologies currently supported:

TOPOLOGY NAME	EXAMPLE	DESCRIPTION	SUPPORTED
---------------	---------	-------------	-----------

TOPOLOGY NAME	EXAMPLE	DESCRIPTION	SUPPORTED
Mixed 1	 <p>Users homed/mailboxes located: EXO and SFB</p>	MA is not enabled for SFB; no SFB MA features available in this topology.	No MA features for SFB.
Mixed 2	 <p>Users homed/mailboxes located: EXCH and SFBO</p>	MA is on for SFBO only. The authorization server is Azure AD for users homed in SFBO, but AD for EXCH on-premises.	MFA, CBA, CA/MAM with Intune.*
Mixed 3	 <p>Users homed/mailboxes located: EXO + SFB, or EXCH + SFB</p>	No SFB MA features available in this topology	No MA features for SFB.
Mixed 4	 <p>Users homed/mailboxes located: EXCH + SFBO or EXCH + SFB</p>	MA is on for SFBO, therefore the authorization server is Azure AD for users homed in SFBO. On-prem users in SFB and EXO use AD.	MFA, CBA, CA/MAM with Intune for online users only.*
Mixed 5	 <p>Users homed/mailboxes located: EXO + SFBO, EXO + SFB, EXCH + SFBO, or EXCH + SFB</p>	MA is on in both EXO and SFBO, therefore the authorization server is Azure AD for users homed in SFBO; on-prem users in EXCH and SFB use AD.	MFA, CBA, CA/MAM with Intune for online users only.*
Mixed 6	 <p>Users homed/mailboxes located: EXO + SFBO, EXO + SFB, EXCH + SFBO, or EXCH + SFB</p>	MA is on everywhere, therefore the authorization server is Azure AD for all users. (online and on-premises) Please see <a href="https://aka.ms/ModernAuthOverview">https://aka.ms/ModernAuth Overview</a> for deployment steps.	MFA, CBA and CA/MAM (via Intune) for all users.

\* - MFA includes Windows Desktop, MAC, iOS, Android devices, and Windows Phones; CBA includes Windows Desktop, iOS and Android devices; CA/MAM with Intune, includes Android and iOS devices.

**IMPORTANT**

It's very important to note that users may see **multiple prompts** in some cases, notably where the MA state is not the same across all the server resources that clients may need and request, as is the case with all versions of the Mixed topologies.

**IMPORTANT**

Also note that in some cases (Mixed 1, 3, and 5 specifically) an [AllowADALForNonLynIndependentOfLync](#) registry key must be set for proper configuration for Windows Desktop Clients.

# Manage server-to-server authentication (OAuth) and partner applications in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Manage OAuth and partner applications in Skype for Business Server.

Skype for Business Server must be able to securely, and seamlessly, communicate with other applications and server products. For example, you can configure Skype for Business Server so that contact data and/or archiving data is stored in Microsoft Exchange Server 2013; however, this can only be done if Skype for Business Server and Exchange are able to securely communicate with one another. Likewise, you can schedule a Skype for Business Server conference from within Office Web Apps Server; again, this can only be done if the two servers (SharePoint and Skype for Business Server) trust one another. Although it's possible to use one authentication mechanism for communication between Skype for Business Server and Exchange but a separate mechanism for Skype for Business Server and SharePoint communication, a better and more efficient approach is to use a standardized method for all server-to-server authentication and authorization.

Using a single, standardized method for server-to-server authentication is the approach taken by Skype for Business Server. Started with Office Servers 2013 release, Skype for Business Server (as well as other Microsoft Server products, including Exchange Server and SharePoint Server) supported the OAuth (Open Authorization) protocol for server-to-server authentication and authorization. With OAuth, a standard authorization protocol used by a number of major websites, user credentials and passwords are not passed from one computer to another. Instead, authentication and authorization is based on the exchange of security tokens; these tokens grant access to a specific set of resources for a specific amount of time.

OAuth authentication typically involves three parties: a single authorization server and the two realms that need to communicate with one another. (You can also do server-to-server authentication without using an authorization server, a process that will be discussed later in this document.) Security tokens are issued by the authorization server (also known as a security token server) to the two realms that need to communicate; these tokens verify that communications originating from one realm should be trusted by the other realm. For example, the authorization server might issue tokens that verify that users from a specific Skype for Business Server realm are able to access a specified Exchange realm, and vice-versa.

## NOTE

A realm is simply a security container. By default, Skype for Business Server uses your default SIP domain as its OAuth realm. Additional SIP namespaces are added to the Subject Alternate Name list in the OAuth certificate.

Skype for Business Server supports three server-to-server authentication scenarios. With Skype for Business Server, you can:

- Configure server-to-server authentication between an on-premises installation of Skype for Business Server and an on-premises installation of Exchange and/or SharePoint Server.
- Configure server-to-server authentication between a pair of Office 365 components (for example, between Microsoft Exchange Server and Skype for Business Server, or between Skype for Business Server and SharePoint).
- Configure server-to-server authentication in a cross-premises environment (that is, server-to-server authentication between an on-premises server and an Office 365 component).

Note that, at this point in time, only Exchange 2013, SharePoint Server, Lync Server 2013, Skype for Business

Server 2015, and Skype for Business 2019 support server-to-server authentication; if you are not running one of these servers, you will not be able to fully implement OAuth authentication.

It should also be pointed out that server-to-server authentication is optional: If Skype for Business Server does not need to communicate with other servers (such as Exchange) then server-to-server authentication can be skipped altogether. If server-to-server authentication is already configured for Lync Server 2013 and other applications, there's no need to re-do it for Skype for Business Server.

However, server-to-server authentication is required if you want to use some of the features in Skype for Business Server, such as the "unified contact store." With unified contact store, Skype for Business Server contact information is stored in Exchange instead of in Skype for Business Server; this enables users to have a single set of contacts that is readily accessible from within Skype for Business, Outlook, or Outlook Web Access. Because the unified contact store requires Skype for Business Server to share information with Exchange, you must use server-to-server authentication in order to deploy the feature. Server-to-server authentication is also required if you choose to use Exchange archiving, in which the transcripts of instant messaging sessions are saved as Exchange emails rather than as individual database records.

For the Office 365 version of Skype for Business Server to communicate with its Exchange counterpart, Skype for Business Server must first obtain a security token from the authorization server. Skype for Business Server then uses that security token to identify itself to Exchange. The Office 365 version of Exchange must go through the same process in order to communicate with Skype for Business Server.

However, for on-premises server-to-server authentication between two Microsoft servers there is no need to use a third-party token server. Server products such as Skype for Business Server and Exchange have a built-in token server that can be used for authentication purposes with other Microsoft servers (such as SharePoint Server) that support server-to-server authentication. For example, Skype for Business Server can issue and sign a security token by itself, then use that token to communicate with Exchange. In a case like this, there is no need for a third-party token server.

In order to configure server-to-server authentication for an on-premises implementation of Skype for Business Server, you must do two things:

- Assign a certificate to the built-in Skype for Business Server token issuer.
- Configure the server that Skype for Business Server will communicate with to be a "partner application." For example, if Skype for Business Server needs to communicate with Exchange, you will need to configure Exchange to be a partner application.

#### **NOTE**

A "partner application" is any application that Skype for Business Server can directly exchange security tokens with, without having to go through a third-party security token server.

Note that OAuth is a core part of the product and cannot be disabled or removed.

## See also

[Assign a server-to-server authentication certificate to Skype for Business Server](#)

[Configure a hybrid environment in Skype for Business Server](#)



# User and client authentication for Skype for Business Server

5/20/2019 • 3 minutes to read

A trusted user is one whose credentials have been authenticated by a trusted server in Skype for Business Server. This server is usually a Standard Edition server, Enterprise Edition Front End Server, or Director. Skype for Business Server relies on Active Directory Domain Services as the single, trusted back-end repository of user credentials.

Authentication is the provision of user credentials to a trusted server. Skype for Business Server uses the following authentication protocols, depending on the status and location of the user.

- **MIT Kerberos version 5 security protocol** for internal users with Active Directory credentials. Kerberos requires client connectivity to Active Directory Domain Services, which is why it cannot be used for authenticating clients outside the corporate firewall.
- **NTLM protocol** for users with Active Directory credentials who are connecting from an endpoint outside the corporate firewall. The Access Edge service passes logon requests to a Director, if present, or a Front End Server for authentication. The Access Edge service itself performs no authentication.

## NOTE

NTLM protocol offers weaker attack protection than Kerberos, so some organizations minimize usage of NTLM. As a result, access to Skype for Business Server might be restricted to internal or clients connected through a VPN or DirectAccess connection.

- **Digest protocol** for so-called anonymous users. Anonymous users are outside users who do not have recognized Active Directory credentials but who have been invited to an on-premises conference and possess a valid conference key. Digest authentication is not used for other client interactions.

Skype for Business Server authentication consists of two phases:

1. A security association is established between the client and the server.
2. The client and server use the existing security association to sign messages that they send and to verify the messages they receive. Unauthenticated messages from a client are not accepted when authentication is enabled on the server.

User trust is attached to each message that originates from a user, not to the user identity itself. The server checks each message for valid user credentials. If the user credentials are valid, the message is unchallenged not only by the first server to receive it but by all other servers in the trusted server cloud.

Users with valid credentials issued by a federated partner are trusted but optionally prevented by additional constraints from enjoying the full range of privileges accorded to internal users.

The ICE and TURN protocols also use the Digest challenge as described in the IETF TURN RFC.

Client certificates provide an alternate way for users to be authenticated by Skype for Business Server. Instead of providing a user name and password, users have a certificate and the private key corresponding to the certificate that is required to resolve a cryptographic challenge. (This certificate must have a subject name or subject alternative name that identifies the user and must be issued by a Root CA that is trusted by servers running Skype for Business Server, be within the certificate's validity period, and not have been revoked.) To be authenticated,

users only need to type in a personal identification number (PIN). Certificates are particularly useful for telephones, mobile phones, and other devices where it is difficult to enter a user name and password.

### **Cryptographic requirements due to ASP .NET 4.5**

As of Skype for Business Server 2015 CU5, AES is not supported for ASP.NET 4.6 and this may cause Skype Meetings App to fail to start. If a client is using AES as the machine key validation value you will need to reset the machine key value to SHA-1 or another supported algorithm on the Skype Meetings App site level on IIS. If necessary, see [IIS 8.0 ASP.NET Configuration Management](#) for instructions.

Other supported values are:

- HMACSHA256
- HMACSHA384
- HMACSHA512

The values AES, 3DES, and MD5 are no longer allowed, as they once were in ASP.NET 4. [Cryptographic Improvements in ASP.NET 4.5, pt. 2](#) has more details.

# Plan for clients and devices

5/20/2019 • 9 minutes to read

**Summary:** Review of the supported clients and apps for Skype for Business.

Today's workforce is constantly on the move. Employees need to communicate and collaborate whether working from the corporate office, at regional locations, in home offices, or on the road. Skype for Business Server supports these needs through a collection of client interfaces that you can deploy to your organization's users. Thoughtful planning ensures that employees get what they need and that Skype for Business is available to them wherever they happen to be.

## Available clients

Skype for Business Server supports several types of clients, including computer-installed client software, web-based clients, and clients for mobile devices. The primary clients are introduced in this section, for a detailed listing of all supported clients see either [Desktop client feature comparison for Skype for Business Server 2015](#) or [Desktop client feature comparison for Skype for Business Server 2019](#). If you've previously used a combination of Lync clients, note that there are unsupported [Legacy clients](#) that are incompatible with Skype for Business Server 2019. Updates take place regularly so check this topic periodically for the latest client information.

### Skype for Business (2019)

Skype for Business (2019) is the recommended full-featured client for Skype for Business Server 2015 and 2019. See [Follow the latest updates in Skype for Business](#) for a description of new features. Client feature support is detailed in the [Desktop client feature comparison for Skype for Business](#), and user documentation is at [Skype for Business help](#). This client is included when a user installs Office 365.

A free basic client supporting fewer features is also available. Both versions are available for download at [Download Skype for Business across all your devices](#). The differences between Full and Basic clients are described in the [Basic client limitations](#) section.

### Skype for Business 2016

Skype for Business 2016 is a full-featured client for Skype for Business Server 2015 or 2019. See [What's new in Skype for Business 2016](#) for a description of new features. Client feature support is detailed in the [Desktop client feature comparison for Skype for Business](#), and user documentation is at [Skype for Business help](#). This client is included when a user installs Office 365.

A free basic client supporting fewer features is also available. Both versions are available for download at [Download Skype for Business across all your devices](#). The differences between Full and Basic clients are described in the [Basic client limitations](#) section.

### Skype for Business 2015

Skype for Business 2015 is a full-featured client for Skype for Business Server 2015 or 2019. The Skype for Business user interface has been fully redesigned and includes newly integrated features, such as Call Monitor, Skype directory integration, emoticons, and more. For a summary of changes, see [Lync is now Skype for Business — see what's new](#). Client feature support is detailed in the [Desktop client feature comparison for Skype for Business](#), and user documentation is at [Skype for Business help](#). This client is included when a user installs Office 365.

### Skype for Business on Mac

The [Skype for Business on Mac](#) client is available for download. See [Skype for Business on Mac client requirements](#) to review prerequisites.

## Skype for Business for mobile devices

Clients are available for Windows Phone, iPhone/iPad, and Android. Users can get them at [Download Skype for Business across all your devices](#). Feature support for these clients is detailed in [Mobile client feature comparison for Skype for Business](#).

### NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## Online Meeting Add-in for Skype for Business

The Online Meeting Add-in for Skype for Business supports meeting management from within Microsoft Outlook messaging and collaboration client on Windows. The Online Meeting Add-in for Skype for Business software installs automatically with Skype for Business.

## Skype for Business Web App and Skype Meetings App

If Skype for Business is not installed on a user's computer and the user clicks a meeting link in a meeting request on a Windows computer, the Skype Meetings App or Skype for Business Web App will be installed and open. Skype Meetings App is the client of choice for participants outside your organization. (Note that on a Mac, Skype for Business on Mac will be installed and open.) See [Plan for Meetings clients \(Web App and Meetings App\)](#) for the requirements to use these clients.

## Skype for Business Web Scheduler

[Skype for Business Web Scheduler](#) is a web-based meeting scheduling and management tool for users of Skype for Business Online who don't have access to Microsoft Outlook, or who are on an operating system not based on Windows. With Skype for Business Web Scheduler, users can create new meetings, modify existing meetings, and send invitations using their preferred email program. Skype for Business Web Scheduler [documentation](#) provides further details.

## VDI plugins

A Virtual Desktop Infrastructure (VDI) environment is used in some organizations where security and compliance issues are especially sensitive. Using Skype for Business with full audio and video on a connection like that requires heavy loads of audio and video processing on the client homed on a virtual desktop. Additional VDI plugin software is available that offloads that processing to the end user's local machine, and reduces the load on the virtual desktop. See [Plan for Skype for Business in VDI environments](#) for details on using these plugins.

## Microsoft Teams Rooms

Microsoft Teams Rooms is Microsoft's latest conferencing solution which uses a familiar interface and is easily deployed and managed, leveraging existing equipment like LCD panels for ease of installation. Microsoft Teams Rooms uses a purpose-built UWP app running on a Surface Pro 4 or Surface Pro in a console mode (once deployed the UWP app is the only app that will run on the device) and it requires its own device account on your implementation. Software is updated via both Windows store and Windows Update. See <https://aka.ms/MTRDocs> for details on using these room consoles in your deployment.

## Skype for Business on Surface Hub

Microsoft Surface Hub is an all-in-one productivity device that is intended for brainstorming, collaboration, and presentations. It has its own iteration of the Skype for Business client, documented in the [Microsoft Surface Hub admin guide](#).

# Choosing your organization's preferred client

If your organization bought the appropriate licenses, choose the Full client, otherwise choose the Basic client.

Your users can install the client for themselves from [Download Skype for Business across all your devices](#). The client is also installed when users install Office 365 on Windows. If some of your users have Macs, those users will have a different set of features as described in earlier sections.

Some features available with Skype for Business Server 2015 are not available in Skype for Business Online or Skype for Business Server 2019, see [Online or Hybrid user account limitations for 2015](#) or [Online or Hybrid user account limitations for 2019](#) for specifics. Skype for Business Online Admins may want to refer to [Skype for Business Online Service Description](#) for information on the different plans available to them.

Before you deploy or upgrade to Skype for Business, check which clients are already in use in your organization. Use the [Desktop client feature comparison for Skype for Business](#) to understand the feature support impact on those clients. This can help you communicate changes to users, pace the roll-out process, and fully understand the benefits of upgrading to the latest client.

## Ways to deploy the client to your users

Client installers are available for both MSI and click-to-run type installers. The Skype for Business client-sustainment strategy may affect your choices, so you should understand the following points:

- In general Skype for Business does NOT add new features to previously released clients
- In general Skype for Business does NOT plan on shipping new features in the Skype for Business MSI after its initial release. MSI improvements between releases will primarily be quality/security in nature.
- The latest and greatest Skype for Business client experience will be found in the Skype for Business 2019 click-to-run installer.

You can do a customized deployment of the client as described in [Customize Windows client installation in Skype for Business Server](#). Installation methods are described in greater detail in [Deploy clients for Skype for Business Server](#)

### Click-to-run

Click-to-run is a Microsoft streaming and virtualization technology that you can use to install and update Office products including Skype for Business. These streaming and virtualization capabilities are based on technologies in Microsoft Application Virtualization (App-V). Click-to-run has the following advantages:

- Streamed installation of Office suite that results in short installation time
- Slipstreamed Updates and patches
- Takes up less disk space
- User-base licensing: 5 installs per user
- Customizable via XML Editor for the installation of independent programs

You may want to use the [Office Deployment Tool](#) for this type of installer.

Both the basic and full client versions (with choice of 32- and 64-bit versions) are available using a click-to-run installer, your users can download at [Download Skype for Business across all your devices](#).

### MSI

MSI is a more traditional installation method, used on the Skype for Business 2015 and 2016 clients. It allows you to manually install updates and patches, use volume licensing and activation, and is customizable via the [Office Customization Tool](#). You can distribute clients by applying Group Policies, by using System Center Configuration Manager, or using a third party tool.

## Legacy clients

Skype for Business Server 2019 and Skype for Business Online support the following previously released clients: Skype for Business 2016, Skype for Business 2015, Lync 2013.

Skype for Business Server 2015 supports the following previously released clients: Lync 2013, Lync 2010, Lync 2010 Mobile, Lync Phone Edition, and Lync 2010 Attendant. For information about these clients when used with other servers, see the [Client comparison tables for Lync Server 2013](#) and [Client comparison tables for Lync Server 2010](#).

## Client system requirements

See the following articles to understand the supported features, platforms, operating systems, browsers, and integration required for Skype for Business clients.

- [Plan the Skype for Business client experience for your users](#)
- [Desktop client feature comparison for Skype for Business](#)
- [Mobile client feature comparison for Skype for Business](#)
- [Windows client requirements and software support](#)
- [Skype for Business compatibility with Office apps](#)
- [Skype for Business client video resolutions](#)
- [Plan for Meetings clients \(Web App and Meetings App\)](#)
- [System requirements for Skype for Business for Windows Phone](#)
- [Skype for Business on Mac client requirements](#)
- [Plan for Microsoft Teams Rooms](#)
- [Plan for Skype for Business in VDI environments](#)
- Refer to the [System requirements](#) for the required hardware.

## See also

[Latest updates for versions of Skype for Business that use Windows Installer \(MSI\)](#)

# Plan the Skype for Business 2015 client experience for your users

5/20/2019 • 10 minutes to read

**Summary:** Learn about the new Skype for Business and the steps you can take to prepare your environment and your users for the update, whether you're using Skype for Business Online, Skype for Business Server 2019, Skype for Business Server 2015, Lync Server 2013, or Lync Server 2010.

The April 14th, 2015 Office Update for Lync 2013 includes the new Skype for Business user interface. This update enables administrators to control the look and feel of the client and choose whether to retain the Lync 2013 client experience or use the improved Skype for Business client experience. The Skype for Business client effectively replaced the Lync 2013 client, and added the ability for administrators to choose between the existing Lync client experience and the new Skype for Business client experience. For information about this update, see [April 14, 2015 update for Lync 2013 \(Skype for Business\) \(KB2889923\)](#).

On May 12th, 2015 there will be another monthly update from Office that includes the updated Skype for Business client. Many customers that did not apply the April update will pick up the May 12th update for Office 2013. The information in this topic will help you prepare your organization, your environment, and your users for the client update. To make the transition easy for your users and support teams, use the information in this topic to help you decide which client experience you want for your users and then make the changes to your environment before deploying the client update in your organization.

- [What client experience do you want for your users?](#)
- [Prepare your environment for the Skype for Business client](#)
- [Resources to help you prepare your support teams and your end users for the update](#)

## NOTE

The Lync 2013 client experience is not an option for Skype for Business 2016 client versions. Before you attempt to configure your client environment to use the Lync 2013 client, please check the client version to ensure it does not start with the number 16; for example: 16.x.x.x.

## What client experience do you want for your users?

With the new Skype for Business client, you can control which client experience your users get, either Lync or Skype for Business. The default client experience depends on whether you are using Lync or Skype for Business on-premises or online. If you are using Skype for Business Online (Lync Online) today with Office 365 ProPlus, Office 365 Business Premium or Office 2013, the updated Skype for Business client experience—inspired by the look and feel of Skype—will be the default user experience. If you are using Lync Server on-premises today, the Lync client experience will be the default.

You can configure which client experience your users get by using client policies. A client policy is a set of configuration settings that are applied to users when they login to Lync or Skype for Business.

### Skype for Business client experience

In addition to all the features of Lync, Skype for Business provides new features with simplified controls and familiar icons from Skype. Some new features in Skype for Business are available only with the new Skype for Business client experience. To learn more about the new features in Skype for Business, see [Discover Skype for](#)

Business.

## Lync client experience

The Lync client experience is very similar to the Lync 2013 client experience that your users are already familiar with, but there are a few changes that you'll want to let your users know about. To see what's different between the Lync client experience and the Lync 2013 client, see [Why do I see Skype for Business when I'm using Lync?](#) and the additional links later in this topic.

## Prepare your environment for the Skype for Business client

There are a few things you'll need to do to get your environment ready for the client update. Before you start making any changes to configure the client experience, you first need to make sure that you are using a version of Skype for Business Server or Lync Server that supports the client policy settings.

Once you've confirmed that you're using a version of Skype for Business Server or Lync Server that supports the policy settings to control the client experience, you'll need to configure the policy settings in your environment. The specific steps you need to follow depend on the version of Skype for Business Server or Lync Server that you are using, and whether your users are on-premises or online.

You'll want to make these changes before the client update is delivered to your users so that you can control the client experience from the first time they start the Skype for Business client. The following tables points you to the steps you need to take to configure your environment for the desired client experience for your users.

DEPLOYMENT	SKYPE FOR BUSINESS CLIENT EXPERIENCE	LYNC CLIENT EXPERIENCE
Skype for Business Online	There are no additional steps other than to deploy client build 4711.1002 (April, 2015) or later.	<a href="#">Use the Lync client experience with Skype for Business Online</a>
Skype for Business Server 2015	There are no additional steps other than to deploy client build 4711.1002 (April, 2015) or later.	<a href="#">Use the Lync client experience with Skype for Business Server on-premises</a>
Lync Server 2013 and Lync Server 2010	<a href="#">Use the Skype client experience with Lync Server 2013 or Lync Server 2010 on-premises</a>	<a href="#">Use the Lync client experience with Lync Server 2013 or Lync Server 2010 on-premises</a>

## Use the Skype client experience with Lync Server 2013 or Lync Server 2010 on-premises

Follow the steps in this section if you want to configure the Skype client experience in an on-premises deployment. The default experience for on-premises

**Step 1:** First, make sure you are running a version of Lync Server that supports the client policy settings.

- **Lync Server 2013** - You must be running the December 2014 Cumulative Update (5.0.8308.857) for Lync Server 2013 or a later update. For information, see [Updates for Lync Server 2013](#).
- **Lync Server 2010** - You must be running the February 2015 Cumulative Update (4.0.7577.710) for Lync Server 2010 or a later update. For information, see [Updates for Lync Server 2010](#).

**Step 2:** Next, use a client policy to set the Skype client experience with the Skype for Business client. There are **3 options** for using a client policy to set the client experience.

**Option 1:** Set the Skype client experience by using a Global policy. Note that the Global policy applies to all of the users in your deployment, but user and site level policies take precedence over the Global policy:



```
Set-CsClientPolicy -Identity Global -EnableSkypeUI $True
```

**Option 2:** Modify an existing client policy that you are using in your environment to include the setting to enable the Skype client experience. This lets you assign the Skype client experience only to those users that have the existing policy assigned:

```
Set-CsClientPolicy -Identity ExistingClientPolicyName -EnableSkypeUI $True
```

**Option 3:** Create a new policy to assign to users that includes the setting for the Skype client experience. First, create the new client policy and provide the name of the policy as the value of the **Identity** parameter:

```
New-CsClientPolicy -Identity UseSkypeUI -EnableSkypeUI $True
```

Then assign the policy to users, using the name of the policy (the value you used for the **Identity** parameter) as the value of the **PolicyName** parameter:

```
Grant-CsClientPolicy username@contoso.com -PolicyName UseSkypeUI
```

**Step 3:** After you've configured your client policies, deploy the Skype for Business client, build 4711.1002 (April, 2015) or later.

## Use the Lync client experience with Lync Server 2013 or Lync Server 2010 on-premises

This is the default experience when the Skype for Business client is deployed in an on-premises Lync Server deployment. You don't need to configure any client policies to use the Lync client experience, but you may want to control the first run behavior for the client. By default, the first time users start the Skype for Business client, the Skype client experience is used and a notification is displayed to users that requests that they restart the client to get the Lync client experience. You can configure your environment so that the Lync client experience is displayed the first time users start the client, as well as turn off the client tutorial by modifying the system registry on client computers. For the steps you need to perform before you deploy the Skype for Business client, see one of the following topics:

- **Lync Server 2013**, see [Configure the client experience with Skype for Business in Lync Server 2013](#)
- **Lync Server 2010** see [Configure the client experience with Skype for Business in Lync Server 2010](#)

## Use the Lync client experience with Skype for Business Server on-premises

Follow the steps in this section if you want to configure the Lync client experience in an on-premises Skype for Business Server deployment.

Follow the steps in this section if you want to configure the Skype client experience in an on-premises deployment. The default experience for on-premises

**Step 1:** First, deploy Skype for Business Server.

**Step 2:** Next, use a client policy to set the Lync client experience with the Skype for Business client. There are **3 options** for using a client policy to set the client experience.

**Option 1:** Set the Lync client experience by using a Global policy. Note that the Global policy applies to all of the

users in your deployment, but user and site level policies take precedence over the Global policy:

```
Set-CsClientPolicy -Identity Global -EnableSkypeUI $False
```

**Option 2:** Modify an existing client policy that you are using in your environment to include the setting to enable the Lync client experience. This lets you assign the Lync client experience only to those users that have the existing policy assigned:

```
Set-CsClientPolicy -Identity ExistingClientPolicyName -EnableSkypeUI $False
```

**Option 3:** Create a new policy to assign to users that includes the setting for the Lync client experience. First, create the new client policy and provide the name of the policy as the value of the **Identity** parameter:

```
New-CsClientPolicy -Identity UseLyncUI -EnableSkypeUI $False
```

Then assign the policy to users, using the name of the policy (the value you used for the **Identity** parameter) as the value of the **PolicyName** parameter:

```
Grant-CsClientPolicy username@contoso.com -PolicyName UseLyncUI
```

**Step 3: Optional** - By default, the first time users start the Skype for Business client, the Skype client experience is used and a notification is displayed to users asking them to restart the client to get the Lync client experience. You can configure your environment so that the Lync client experience is displayed the first time users start the client, as well as turn off the client tutorial, by modifying the system registry on client computers. For the steps you need to perform before you deploy the Skype for Business client see [Configure the client experience with Skype for Business](#).

**Step 4:** After you've configured your client policies, deploy the Skype for Business client, build 4711.1002 (April, 2015) or later.

## Use the Lync client experience with Skype for Business Online

Follow the steps in this section if you want to configure the Lync client experience and you using Skype for Business Online.

If you are using Skype for Business Online, you can still use the Lync client experience with the Skype for Business client in your organization by using Remote PowerShell to configure client policies. There are **3 options** for using a client policy to set the client experience. Note that the policy and parameter names are different than the settings you use to configure the client experience when you are using Skype for Business or Lync Server on-premises.

**Option 1:** Set the Lync client experience by using a Global policy. Note that client and site policies applied to users will take precedence over a Global policy.

```
Grant-CsClientPolicy -PolicyName ClientPolicyDisableSkypeUI
```

**Option 2:** Modify an existing client policy that you are using in your environment to include the setting to enable the Lync client experience. This lets you assign the Lync client experience only to those users that have the existing policy assigned:

```
Grant-CsClientPolicy -PolicyName ClientPolicyDisableSkypeUI
```

**Option 3:** Use a custom policy instance that includes the setting for the Lync client experience.

```
Grant-CsClientPolicy username@contoso.com -PolicyName ClientPolicyNoIMURLDisableSkypeUI
```

After you've configured your client policies, deploy the Skype for Business client, build 4711.1002 (April, 2015) or later.

For detailed information about how to configure the client experience with Skype for Business Online, including steps about how to control the first run experience and PowerShell scripts you can use to configure your environment, see [Switching between the Skype for Business and the Lync client user interfaces](#).

## Resources to help you prepare your support teams and your end users for the update

To make it easier for you and your organization prepare for the transition, we have many additional resources available to help you plan, educate and engage end-users.

- [Video: Introducing Skype for Business](#)
- [Skype for Business Quick Start Guides \(Download\)](#)
- [Lync is now Skype for Business — see what's new](#)
- [Skype for Business: Step-by-step guide for new users](#)
- [Why do I see Skype for Business when I'm using Lync?](#)

# Desktop client feature comparison for Skype for Business Server 2019

5/20/2019 • 10 minutes to read

**Summary:** Skype for Business Server 2019 or Skype for Business Online administrators can use these tables to understand what features are supported on which clients.

Before you deploy or upgrade to Skype for Business Server, check which clients are already in use in your organization. Use the tables below to understand the feature support impact on those clients. This can help you communicate changes to users, pace the roll-out process, and fully understand the benefits of upgrading to the latest client.

Some features available with Skype for Business Server 2019 are not available in Skype for Business Online; see [Online or Hybrid user account limitations](#) for specifics. Skype for Business Online Admins may want to refer to [Skype for Business Online Service Description](#) for information on the different plans available to them.

The following tables show the features that are available with each client that works with Skype for Business Server 2019 or Skype for Business Online. You may also want to refer to [Mobile client feature comparison for Skype for Business](#) for smart phone and tablet client feature comparisons. The Client Access License or User Subscription License your organization purchases will also have an impact on which features are available to your users. Whether you deploy the Full or Basic client to users depends on the license or plan your organization chooses to buy. See the [Licensing Guide](#) for more details.

## IMPORTANT

Skype for Business Server 2019 and Skype for Business Online support the following previously released clients: Lync 2013, Skype for Business 2015, and Skype for Business 2016, as well as the Skype for Business 2019 client. For information about these clients when used with other servers, see the [Client comparison tables for Lync Server 2013](#) and [Desktop client feature comparison for Skype for Business 2015](#).

## NOTE

The Skype for Business Web App browser client and Skype Meetings App Windows 10 app only provide [Meetings support](#). Refer to [Plan for Meetings clients \(Web App and Meetings App\)](#) for more about these clients.

## Enhanced Presence support

This table covers the Enhanced Presence features that extend beyond a simple indication of whether a user is online, offline, busy, etc.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Publish status	✓	✓ ①	✓
View status	✓	✓	✓
View status notes and Out of Office messages	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Add a custom location	✓	✓	✓
Add a custom note	✓	✓	✓
Use a photo from any public site for My Picture (not available in Skype for Business Online)	✓		✓

❶ Does not support publishing status based on calendar free/busy information.

## Contacts and Contact Groups support

This table covers the features relating to managing IM and Presence contacts.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Pre-populated Contacts list	✓		
View and Modify Contacts list	✓	✓	✓
Tag contacts for status change alerts	✓	✓	✓
Control privacy relationships	✓		✓
Search the corporate address book	✓	✓	✓
Search Microsoft Outlook contacts	✓	✓	✓
Manage contact groups	✓	✓	✓
Expand distribution groups and Office 365 Groups	✓	✓	✓
Search for Response Groups (not available in Skype for Business Online)	✓		✓
Display recent contacts group	✓		✓
Display current conversations group	✓	✓	✓
Display alternate contact views (for example, tile)	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Sort contacts by Group, Relationship, or New (people who've added you to their Contacts list)	✓		✓
Sort contacts by Status (availability)	✓		✓
Search and add Exchange contacts	✓		✓

## IM support

This table covers features related to IM support.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Initiate IM with or email to a contact	✓	✓	✓
Navigate among multiple IM conversations/Track multiple conversations in a single tabbed window	✓	✓	✓
Log IM conversations in Outlook	✓	✓ If server-side conversation history is turned on	✓
Check spelling	✓	✓	
Skill search (with SharePoint Server integration) (On-premises Skype for Business Server and on-premises SharePoint 2013 are required for skill search.)	✓		✓
Persistent Chat (Group Chat) integration (not available for Skype for Business Online)	✓		✓
Escalate a Persistent Chat room to a Skype for Business Meeting with one click (not available for Skype for Business Online)	✓		✓
Inline pictures of sender and receiver in IM window	✓		✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Receive ink messages	✓		✓
Set IM messages as high importance	✓		✓

## Meetings support

This table covers features related to Meetings support.

### NOTE

Skype for Business meeting features aren't available in Skype for Business Online Standalone Plan 1. Plan 1 is being [retired](#).

In Skype-to-Skype sessions, a Skype for Business Online Plan 1 user can participate in desktop sharing and application sharing if they're invited by a user who has access to sharing features. For details, see the [Skype for Business Online Service Description](#).

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2016 CLIENT	SKYPE FOR BUSINESS ON MAC	SKYPE FOR BUSINESS WEB APP	SKYPE FOR BUSINESS 2015 CLIENT	LYNC 2013 CLIENT
Add computer audio	✓	✓	✓(requires plug-in)	✓	✓
Add video	✓	✓	✓(requires plug-in)	✓	✓
View multiparty video (gallery view)	✓	✓	✓	✓	✓
Video-based screen sharing	✓	✓	✓ View-only		
Use in-meeting presenter controls	✓	✓	✓	✓	✓
Access detailed meeting roster	✓	✓	✓	✓	✓
Participate in multiparty IM	✓	✓	✓	✓	✓
Share the desktop (if enabled)	✓	✓ ①	✓ ① (requires plug-in)	✓	✓
Share a program (if enabled)	✓	View only	✓(requires plug-in)	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2016 CLIENT	SKYPE FOR BUSINESS ON MAC	SKYPE FOR BUSINESS WEB APP	SKYPE FOR BUSINESS 2015 CLIENT	LYNC 2013 CLIENT
Add anonymous participants (if enabled)	✓	✓	✓	✓	✓
Use dial-in audio meetings ②	✓	✓	✓	✓	✓
Initiate a Meet Now meeting	✓	✓		✓	✓
Add and present Microsoft PowerPoint files	✓	③ Annotations not available	✓	✓	✓
Navigate Microsoft PowerPoint files	✓	✓	✓	✓	✓
Add and edit OneNote meeting notes	✓		Edit only (not add)	✓	✓
Use a whiteboard	✓		✓	✓	✓
Conduct polls	✓		✓	✓	✓
Upload files to share with others	✓	✓	✓	✓	✓
Schedule a meeting or conference	Outlook or Skype for Business Web Scheduler	Outlook or Skype for Business Web Scheduler	Skype for Business Web Scheduler	Outlook or Skype for Business Web Scheduler	Outlook or Lync Web Scheduler
Q&A Manager	✓				
Disable attendee video	✓		✓		
Disable meeting IM	✓		✓	✓	✓
Mute Audience	✓	✓	✓	✓	✓
Make everyone an attendee	✓		✓	✓	✓
Produce Skype Meeting Broadcast	✓				



FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2016 CLIENT	SKYPE FOR BUSINESS ON MAC	SKYPE FOR BUSINESS WEB APP	SKYPE FOR BUSINESS 2015 CLIENT	LYNC 2013 CLIENT
Delegate can schedule a meeting on behalf of delegator	✓	✓	✓		
Synchronize delegates between Skype for Business and Outlook	✓		✓	✓	
Set Video Spotlight (lock video)	✓		✓	✓	✓
Give/Take control of screen sharing	✓		✓		

❶ Participants can't control desktops that are shared by Skype for Business on Mac, Lync for Mac 2011, or Communicator for Mac 2011 users. Skype for Business on Mac, Lync for Mac 2011 and Communicator for Mac 2011 users can't control desktops shared by Windows users. This also won't work for Skype for Business Web App on Max OSX.

❷ For Skype for Business Online, this feature requires Microsoft PSTN Conferencing, Exchange Unified Messaging, or a third-party audio conferencing provider.

❸ The Lync for Mac 2011 client cannot view Microsoft Office 2013 PowerPoint presentations when they have been shared in a conference by the Skype for Business Web App.

❹ For Skype for Business 2016 apps, you must be using Click-to-Run, build 16.0.4227 or later.

① For Skype for Business 2015 apps, you must have the September Update, build 15.0.4747 or later.

## Voice (Telephony) support

This table covers features related to voice services support.

### NOTE

Skype for Business Voice (Telephony) features are limited to certain Skype for Business Online subscription plans. For details, see the [Skype for Business Online Service Description](#).

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Initiate a call	✓	✓	✓
Click to call a contact	✓	✓	✓
Transfer a call	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Manage call forwarding	✓	✓	✓ ①
Manage team call settings	✓		✓ ①
Manage delegates	✓	✓	✓ ①
Initiate a call to a Response Group	✓		✓ ①
Support emergency services (E-911)	✓	✓	✓ ①
IM notification to SIP URI(s) for E-911 call	✓	✓	✓
IM notification to distribution list for E-911 call	✓	✓	✓
Connect to voice mail, set up or change greeting	✓	✓	✓ ①
Missed call notification	✓	✓	✓ ①
Make calls on behalf of another contact (manager/delegate scenario)	✓	✓	✓ ①
Handle another's calls if configured as a delegate	✓	✓	✓ ①
Call park	✓		✓ ①
Group call pickup	✓		✓ ①
Location-based routing	✓	✓	✓
Manage Response Group/Team call group	✓		✓

① This feature isn't available in Skype for Business Online.

## External users support

This table covers features related to support for external users homed on the PSTN.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Initiate IM with a public contact	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Initiate IM with a federated contact	✓	✓	✓
Conduct two-party or multiparty calls with external users (not available in Skype for Business Online)	✓	✓	✓

## Recording support

This table covers features related to support for recording meetings.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Client-side recording of audio, video, application sharing, desktop sharing, and uploaded content	✓ ①		✓ ①
Client-side recording of file transfers, shared OneNote pages, and PowerPoint annotations	✓ ②		✓ ②
Select preferred recording resolution	✓		✓

① Recording is unavailable in certain Skype for Business Online standalone plans. Recording requires full Skype for Business client rights.

② Recording of file transfers, shared OneNote pages, and PowerPoint annotations is unavailable in Skype for Business Online.

## Modern Authentication

This table covers features requiring support for modern authentication.

Modern authentication also requires a topology described in [Skype for Business topologies supported with Modern Authentication](#).

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Modern Authentication	✓	✓	✓
Multi-factor Authentication	✓	✓	✓
Cert -Based Authentication	✓(Domain-joined device only)	✓	✓(Domain-joined device only)
Kerberos Authentication	✓		✓

# Archiving, compliance, and logging support

This table covers features related to support for archiving and logging functions.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2015, 2016, OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC	LYNC 2013 CLIENT
Archiving of IM conversations in Outlook Conversation History	✓ ①	✓ If server-side conversation history is turned on	✓ ①
Client-side archiving of audio, video, application sharing, desktop sharing, and uploaded content	✓ ①		✓ ①
Client-side archiving of file transfers, shared OneNote pages, and PowerPoint annotations (unavailable in Skype for Business Online)	✓		✓
Access sign-in logs from Skype for Business icon in the task bar	✓		✓

① For Skype for Business Online users, this feature requires Exchange Online and is controlled by the user's Exchange mailbox In-Place Hold attribute.

## Client limitations

### Basic client limitations

The features below are available using the Full client and are not available with the Basic client:

- Manage team call settings
- Manage delegates
- Make calls on behalf of another contact (manager/delegate scenario)
- Handle another's calls if configured as a delegate
- Manage a high volume of calls
- Initiate a call to a Response Group
- Call park
- Change greeting
- Group call pickup

### Online or Hybrid user account limitations

User accounts can exist either Online or On-premises, and that will affect the features available to that user. Users with accounts on Skype for Business Online will not have access to the following features, even with the Full client:

- Enhanced Presence: Use a photo from any public site for My Picture
- Contacts: Search for Response Groups

- [IM Support: Persistent Chat \(Group Chat\) integration](#)
- [IM Support: Escalate a Persistent Chat room to a Skype for Business Meeting with one click](#)
- [External Users: Conduct two-party or multiparty calls with external users](#)

## See also

[Plan for clients and devices](#)

[Latest updates for versions of Skype for Business that use Windows Installer \(MSI\)](#)

# Mobile client feature comparison for Skype for Business

6/3/2019 • 7 minutes to read

**Summary:** Review the feature support for the mobile client while planning for Skype for Business Server.

This article compares the features and capabilities among Skype for Business mobile clients and the Skype for Business desktop client in the following categories:

- Sign-in, push notifications, and general features
- Enhanced presence
- Contacts and contact groups
- Instant messaging (IM)
- Skype for Business to Skype for Business audio and video
- Conferencing
- Telephony
- External users
- Archiving and compliance
- Modern Authentication

The following tables list the features that are available to Skype for Business users in an on-premises deployment of Skype for Business Server. The same features are also available to Skype for Business Online and Microsoft Office 365 users, unless otherwise indicated in the table footnotes.

## NOTE

For online help and resources for end users, see [Discover Skype for Business](#).

## NOTE

To compare the features available in other Skype for Business clients, see [Desktop client feature comparison for Skype for Business](#).

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## Sign-in, push notifications, and general features

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Skype for Business session remains signed in	✓	✓ ①	✓ ①	✓
Support for push notifications	✓ ③	✓	✓ ④	✓ ④
Account information for multiple users can be cached on the same device	✓			
Screen reader/voice over	✓	✓ ② English only	✓	✓
Use an external keyboard for accessibility	✓		✓	✓
Microsoft Customer Experience Improvement Program support	✓	✓	✓	✓

① On Windows Phone, Skype for Business signs out automatically after a period of inactivity, as follows:

- If the user has enabled push notifications, Skype for Business signs out after 10 days of inactivity.
- If the user has not enabled push notifications, Skype for Business signs out as soon as the user leaves the app.

On iOS devices, Skype for Business signs out automatically after the mobile client has not contacted the server for 10 days due to loss of network connectivity or other issues.

② In app only.

③ Notifications are available when the app is running in the background.

④ Both Google/Android/GCNS and Apple/APNS mobile notification services use HTTPS/TLS encryption for delivery of notifications. The notification payload is handled in plain text while processed by the notification provider.

- Skype for Business for Android receives simple notifications (delivered via GCNS) with no customer data.
- Skype for Business for iOS receives notifications (delivered via APNS) which may include customer data for the call or message.

## Enhanced presence support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Publish and view status	✓	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
View status based on calendar free/busy information	✓	✓	✓	✓
View status notes and Out of Office messages	✓	✓	✓	✓
Add a custom location	✓			
Add a custom note	✓	✓	✓	✓
Publish status based on calendar free/busy information	✓ ①			
Set manual presence state (such as Busy, Do Not Disturb, and so on)	✓	✓	✓	✓

① Skype for Business mobile clients do not update a user's presence based on the user's free/busy calendar information. If a mobile client user is also signed in to the Skype for Business desktop client, the desktop client updates the user's presence based on the user's free/busy calendar information. If the user is signed in to a mobile client only, the user's presence does not update based on free/busy calendar information.

## Contacts and contact groups support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
View Contacts list	✓	✓	✓	✓
View contact groups	✓	✓	✓	✓
View Frequent Contacts group	✓			
Modify Contacts list	✓	✓	✓	✓
Tag contacts for status change alerts	✓			
Control privacy relationships	✓			
Search the corporate address book	✓	✓	✓	✓
Search Contacts list	✓	✓	✓	✓



FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Manage contact groups	✓			✓
Expand distribution groups	✓	✓		✓
Search for Response Groups	✓ ①	✓		✓
Display or hide contact photos	✓	✓		
Pin a contact to your home screen		✓		

① Not available to Skype for Business Online and/or Office 365 users.

## Instant Messaging support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Initiate instant messaging (IM) with a contact	✓	✓	✓	✓
Participate in multiparty IM	✓	✓	✓	✓
Invite others from within the conversation window	✓	✓	✓	✓
Display current conversations	✓	✓	✓	✓
Navigate among multiple IM conversations	✓	✓	✓	✓
Automatically log IM conversations in Exchange	✓	✓	✓	✓
Send an IM conversation as an email message	✓	✓	✓	✓
Initiate an email to a contact	✓	✓	✓	✓
View missed IM invitations	✓	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Vibrate with incoming IM		✓ ①	✓	✓

① This device vibrates every time an IM is received even if the current message in the IM conversation is displayed

## Skype for Business to Skype for Business audio and video

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Skype for Business-to-Skype for Business voice	✓	✓	✓	✓
Skype for Business-to-Skype for Business video	✓	✓	✓	✓

### NOTE

Video on a mobile device requires a WiFi connection by default.

## Conferencing support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Click a link in the meeting reminder to join a video or VoIP meeting	✓	✓	✓	✓
Participate in multiparty IM	✓	✓	✓	✓
Use dial-out conferencing (server calls the mobile device)	✓ ①	✓ ①	✓ ①	✓ ①
Use dial-in audio conferencing	✓	✓	✓	✓
View meeting video	✓	✓	✓	✓
View multiparty video (gallery view)	✓			
Wait in meeting lobby	✓	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Use in-meeting presenter controls	✓			
Access detailed meeting roster for audio conferences	✓	✓	✓	✓
Access detailed meeting roster for IM conferences	✓	✓	✓	✓
Share desktop or program	✓			
View shared desktop or program (VbSS or RDP)	✓	✓ ②	✓ ②	✓ ②
View shared PowerPoint files	✓	✓ ②	✓ ② ③	✓ ② ③
Upload and present PowerPoint files	✓		✓ ②	✓ ②
Use meeting tools (use whiteboard, conduct polls, share files)	✓			
Navigate a list of your meetings	✓	✓	✓	✓
Join a meeting even if you don't have a Skype for Business account	✓	✓	✓	✓
View more information about meeting participants	✓	✓	✓	✓
Start an unscheduled group conversation with multiple participants directly from your client or device	✓	✓	✓	

① For Office 365 users, this feature requires Enterprise Voice, which is part of the E5 license.

② Requires a WiFi connection by default.

③ Viewing embedded video in PowerPoint presentations is not supported.

## Telephony support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
In Skype for Business, tap the call icon to call a contact	✓	✓	✓	✓
Transfer a call	✓	✓	✓	
Consultative Transfer	✓ ③			
Manage call forwarding	✓ ①	✓	✓	✓
Manage team call settings	✓ ①			
Manage delegates	✓ ①			
Initiate a call to a Response Group	✓ ①			
Support emergency services	✓ ②			
Make calls on behalf of another contact (manager/delegate scenario)	✓ ①			
Handle another contact's calls, if configured as a delegate	✓ ①	✓ ①	✓ ①	✓ ①
Use Call via Work	✓ ①	✓	✓	
Access voice mail	✓	✓	✓	
Use the keypad in Skype for Business	✓ ①	✓	✓	

① Available to Skype for Business Online and/or Office 365 E5 users, and users homed on Skype for Business Server or Lync Server 2013 with Enterprise Voice enabled.

② For Skype for Business Online and/or Office 365 users, this feature is supported by Microsoft partners.

③ Windows Desktop client only.

## External user support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Initiate IM with a public contact	✓	✓	✓	✓

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Initiate IM with a federated contact	✓	✓	✓	✓
Conduct two-party calls with external users	✓	✓	✓	✓
Conduct multiparty calls with external users	✓	✓	✓	✓
Use Call via Work to reach a federated contact on their mobile phone by calling their published work number ①		✓	✓	✓

① By default, federated users are assigned the External Contacts privacy relationship. To be able to reach a federated contact on their mobile phone by calling their published work number, the federated contact must manually assign you the Colleagues privacy relationship.

## Address book integration

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Call device address book contacts		✓	✓	✓
Make Skype for Business calls to contacts directly from device address book				✓

## Archiving and compliance support

FEATURE/CAPABILITY	SKYPE FOR BUSINESS DESKTOP CLIENT	WINDOWS PHONE	IOS	ANDROID
Provide client-side archiving	✓			
Provide client-side recording	✓ ①			

① Not available to Skype for Business Online and/or Office 365 users.

## Modern Authentication

This table covers features requiring support for modern authentication.

Modern authentication also requires a topology described in [Skype for Business topologies supported with](#)

## Modern Authentication.

<b>FEATURE/CAPABILITY</b>	<b>SKYPE FOR BUSINESS DESKTOP CLIENT</b>	<b>WINDOWS PHONE</b>	<b>IOS</b>	<b>ANDROID</b>
Modern Authentication	✓	✓	✓	✓
Multi-factor Authentication	✓	✓	✓	✓
Cert -Based Authentication	✓(Domain-joined device only)		✓	✓
Mobile Application Management (via Intune)			✓	✓

# Windows client requirements and software support

5/20/2019 • 2 minutes to read

**Summary:** Review the Windows client support requirements while planning Skype for Business Server.

This section summarizes software required to support the Skype for Business Windows clients. These clients are installed when Office 365 installs, and are also available at [Download Skype for Business across all your devices](#).

## NOTE

The Online Meeting Add-in for Skype for Business, which supports meeting management from within the Outlook messaging and collaboration client, installs automatically with Skype for Business.

## Software Required for Skype for Business client and the Online Meeting Add-in

SYSTEM COMPONENT	SUPPORTED VERSIONS
Windows Operating system	Windows 10 Windows 8.1 Windows 8 Windows 7 operating system Windows Server 2008 R2 or later with latest service pack <b>Note:</b> Skype for Business and the Online Meeting Add-in for Skype for Business are not supported on Windows Vista or Windows XP (any version).
Installation and updates	Administrator rights and permissions
Browser	Microsoft Edge Internet Explorer 11 Internet browser Internet Explorer 10 Internet browser Internet Explorer 9 Internet browser Internet Explorer 8 Internet browser Internet Explorer 7 Internet browser Mozilla Firefox web browser Google Chrome web browser <b>Note:</b> If you are using Skype for Business with Microsoft Exchange Online and your organization has deployed an authenticating HTTP proxy, Internet Explorer 8 or later is required.
Microsoft Office Integration	Outlook 2010 or later
Microsoft Exchange Integration	Microsoft Exchange Server 2010 or later

## Hardware

Refer to the Office 365 [System requirements](#) for the hardware required to run the Skype for Business client.

## Skype Meetings App and Skype for Business Web App

The Skype Meetings App and Skype for Business Web App support specific combinations of operating systems and browsers. For details, see [Plan for Meetings clients \(Web App and Meetings App\)](#).

# Using Mandatory Profiles

If you plan to use the Skype for Business conferencing features, avoid using Active Directory Domain Services mandatory profiles to sign in to the Skype for Business client. Because mandatory profiles are read-only user profiles, the public key infrastructure (PKI) keys that are required for Skype for Business conferencing cannot be saved to the profile.

## System requirements for Skype for Business for Windows Phone

Microsoft Skype for Business for Windows Phone provides instant messaging (IM), enhanced presence, and telephony for users in your organization who are connecting from a smartphone or a Windows Professional mobile device. Mobile devices enable users to extend the reach of Skype for Business. This topic describes planning considerations for Skype for Business for Windows Phone that include identifying prerequisites and technical requirements, required components, and deployment guidance.

### **Skype for Business for Windows Phone Prerequisites**

Following are the Skype for Business for Windows Phone prerequisites.

- Windows Phone 8.1 or later.
- The Windows Phone device must have the latest updates available from Microsoft. For details, see the Windows Phone 8.1 section at [Windows Phone 8 update history](#).
- The device must have 22 MB of available disk space.
- The user must have a voice and data plan from a carrier.

## See also

[Plan for Meetings clients \(Web App and Meetings App\)](#)

[Skype for Business on Mac client requirements](#)

[Download Skype for Business across all your devices](#)

[Office 365 system requirements](#)



# Skype for Business on Mac client requirements

6/25/2019 • 2 minutes to read

Read this topic to learn about hardware, software, and infrastructure requirements for running Skype for Business on a Mac.

The [Skype for Business on Mac Client](#) is available for download.

## Hardware and software requirements for Skype for Business on Mac

The Skype for Business on Mac client requires Mac OS X El Capitan and higher, and uses at least 100MB of disk space. We support the use of all built-in audio and video devices. External devices must be in the [Skype for Business Solutions Catalog](#).

### NOTE

This list is preliminary and some devices may be qualified for Lync, but not supported on Skype for Business on the Mac. Refer to the [System requirements](#) for the minimum hardware required.

### Legacy Mac clients

Skype for Business Server 2015 also supports the following legacy clients on computers that are running Mac OS 10.5.8 or latest service pack or release (Intel-based) operating systems (Mac OS 10.9 operating system is not currently supported). For details about supported features, see [Desktop client feature comparison for Skype for Business](#).

- Microsoft Lync for Mac 2011 (see [Lync for Mac 2011 Deployment Guide](#))
- Microsoft Communicator for Mac 2011 (see [Communicator for Mac 2011 Deployment Guide](#))

These clients are not supported by Skype for Business Server 2019.

## Infrastructure requirements for Skype for Business on Mac

The Skype for Business on Mac client leverages both the Unified Communications Management Platform (UCMP) as well as the Unified Communications Web API (UCWA) that our mobility clients use.

The client has the same requirements as our mobility clients in that you must have an Access Edge Server and Reverse Proxy deployed in a supported configuration.

### Authentication

The Skype for Business on Mac client supports Cert-based authentication, Microsoft Modern Authentication, and Multi-Factor Authentication when deployed and enabled.

### NOTE

Due to a current limitation, the user's Exchange credentials must be the same as their Skype for Business credentials.

### Certificates

Certificates in use on the Access Edge, Reverse Proxy and Front End servers must not use the SHA-512 hash algorithm.

The HTTP Certificate Revocation List must be defined and accessible by the client. For example, we don't support an LDAP entry in the certificate as your Certificate Revocation List.

## DNS

Mobility must be properly deployed for the Skype for Business on the Mac client to function properly. A common failure scenario is to have both of the following DNS entries resolvable on the internal network:

- `lyncdiscoverinternal.<sipdomain>`
- `lyncdiscover.<sipdomain>`

For more information, refer to: [Deploying Mobility in Lync Server 2013](#), and the [Microsoft Lync Server 2010 Mobility Guide](#).

## See also

[DNS requirements for Skype for Business Server](#)

[Frequently Asked Questions](#)

[Known issues](#)

# Skype for Business compatibility with Office apps

5/20/2019 • 2 minutes to read

Understand the ways you can access Skype for Business features from Outlook and other Microsoft Office applications.

This topic describes the compatibility of Skype for Business with various versions of Microsoft Office suites.

## Office and Skype for Business

The following table describes the Skype for Business features that are supported by various versions of Office once Exchange is deployed and integrated as described in [Integrate Skype for Business Server with Exchange Server](#).

### Skype for Business and Microsoft Office Compatibility

FEATURE	MICROSOFT OFFICE 2010	MICROSOFT OFFICE 2013, 2015, AND 2016	OFFICE 2016 FOR MAC <sup>1</sup>
<b>Outlook features</b>			
Customize Outlook meeting invitations (add logo, help URL, disclaimer, footer text)	No	Yes	Yes
Configure meeting option to mute attendee audio and video by default	No	Yes	No
Unified Contact Store for managing Contacts lists across Office and Skype for Business	No	Yes (requires Exchange 2013 or later)	Yes
High-resolution profile pictures	No	Yes (requires Exchange 2013 or later)	Yes
Presence status in the Microsoft Outlook From, To, and Cc fields	Yes	Yes	Yes
Reply with IM or call from the availability menu	Yes (from the contact card)	Yes (from the contact card)	Yes (from the contact card)
Presence status in a meeting request on the Scheduling Assistant tab	Yes	Yes	No
Reply with IM or call from the toolbar or ribbon in a received email message	Yes	Yes	Yes
<b>Other Office apps</b>			

FEATURE	MICROSOFT OFFICE 2010	MICROSOFT OFFICE 2013, 2015, AND 2016	OFFICE 2016 FOR MAC <sup>1</sup>
OneNote shared notes	No	Yes	No
Setup integrated into the Office setup program	No	Yes	No
PowerPoint presentation content	Yes	Yes (VBSS also available)	Yes
IM and presence in Microsoft Word and Microsoft Excel files (smart tags enabled)	Microsoft Word only	Microsoft Word only	No
IM and presence in Microsoft SharePoint sites (Outlook must be installed)	Yes	Yes	No

<sup>1</sup> - Assumes you have installed and are currently running a Skype for Business on Mac client or the Lync 2011 for Mac client.

## Exchange Server and Skype for Business

The following table describes Skype for Business support for various versions of Exchange Server. Outlook must be installed on the client computer to handle Extended MAPI calls, and some features require the use of Exchange Web Services (EWS).

### Skype for Business and Exchange Server Compatibility

EXCHANGE SERVER VERSION	SKYPE FOR BUSINESS SUPPORT
Exchange Server 2019 (Skype for Business Server 2019 only)	Same as Exchange Server 2013 support
Exchange Server 2016	Same as Exchange Server 2013 support
Exchange Server 2013	Same as Exchange Server 2010 support, with the addition of <ul style="list-style-type: none"> <li>Unified Contact Store</li> <li>High-resolution pictures</li> <li>Archiving integration</li> </ul> <b>Note:</b> For details, see <a href="#">Integrate Skype for Business Server with Exchange Server</a> .
Exchange Server 2010 (Skype for Business Server 2015 only)	The following features are available only through EWS: <ul style="list-style-type: none"> <li>Read or delete items in the Conversation History folder</li> <li>Read or delete voice mail items</li> <li>Display extended free/busy information and meeting subject and location</li> <li>Exchange contact sync</li> </ul> Public folders are optional in Exchange Server 2010.

## See also

[Windows client requirements and software support](#)

[Plan for Meetings clients \(Web App and Meetings App\)](#)



# Skype for Business client video resolutions

5/20/2019 • 4 minutes to read

**Summary:** Review the client video requirements while planning for Skype for Business Server.

This article describes video hardware support for Skype for Business video calls and describes how to determine the expected video quality for various computer, tablet, and mobile device configurations.

IT Professionals will find this information useful in assessing the suitability of laptops already in use in their organization, or under consideration for use. They can also search the [Solutions Catalog](#) for information on specific devices.

## Windows desktop, Mac and tablet video requirements and capabilities

Skype for Business uses hardware acceleration for video encoding and decoding based on the H.264/MPEG-4 Part 10 Advanced Video Coding standard. This allows computers with lower CPU clock speeds to encode and decode higher resolution video. Video hardware requirements vary depending on the computer configuration and the video resolution wanted.

Also see [Windows and Mac hardware requirements](#).

### Video hardware requirements

FEATURE	REQUIREMENT
Hardware accelerated H.264 decoding using DirectX Video Acceleration (DXVA)	<ul style="list-style-type: none"><li>• Graphics card must support DirectX 9.0 and must expose the DXVA2_ModeH264_VLD_NoFGT decoding mode and the DirectX 9 API.</li><li>• The latest graphics card driver must be installed.</li></ul>
Hardware accelerated H.264 encoding: Chipset Requirements	<p>The following Intel hardware accelerated video encoding solutions are supported:</p> <ul style="list-style-type: none"><li>• Second- and third-generation Intel HD Graphics 2000, 2500, 3000, and 4000 chipsets (or later versions) with integrated hardware video encoders. Installation of the Intel HD Graphics driver 15.28.9.2884 or the latest driver containing the following is required:</li><li>• Display driver 9.17.10.2884 or the latest driver</li><li>• Hardware media foundation transform (HMFT) version 3.12.10.31 or the latest HMFT</li></ul> <p>The following AMD hardware accelerated video encoding solutions are supported:</p> <ul style="list-style-type: none"><li>• AMD Video Codec Engine, which is available in several discrete graphics cards and in integrated accelerated processing units of AMD A-Series Accelerated Processors. The AMD Video Codec Engine driver 9.12.0.0 or higher must be installed.</li></ul>

FEATURE	REQUIREMENT
Hardware accelerated H.264 encoding: Camera Requirements	<p>USB video cameras with integrated H.264 hardware encoder that conforms to the USB Video Class (UVC) specification version 1.5.</p> <p><b>Note:</b> Skype for Business supports UVC 1.5 cameras with Windows 8 or Windows 8.1, which includes support for UVC 1.5. Because Windows 7 does not include support for UVC 1.5, Skype for Business treats UVC 1.5 cameras as regular cameras with no hardware encoding support.</p>

### Determining H.264 video encoding and decoding capabilities

Generally, there are four major factors that determine the maximum encoding and decoding capability of a particular computer configuration:

- Support for hardware accelerated decoding by using DXVA
- Support for hardware accelerated encoding
- Number of physical cores
- Windows Experience Index (WEI)

The Windows System Assessment Tool (WinSAT) determines the WEI. When you run the WinSAT tool, it generates a Formal.Assessment.XML document on the computer in the %windir%\Performance\WinSAT\DataStore directory. This XML file contains the following two scores that are of particular importance for determining encoding and decoding capabilities:

- The VideoEncodeScore indicates the software-based video encoding capability of the computer.
- The GraphicsScore value indicates the hardware accelerated encoding capability of the computer.

The following three tables explain the maximum encoding and decoding capability for different PC types depending on what hardware acceleration they support. For resolutions of 640x360 and higher, the maximum supported frame rate is 30 frames per second (fps). For resolutions lower than 640x360, the maximum supported frame rate is 15 fps.

### Computer Without DXVA And Without Hardware Accelerated Encoder

CAPABLE ENCODER RESOLUTION	CAPABLE DECODER RESOLUTION	REQUIREMENT
424x240	424x240 (640x360 at 15fps for receive only scenarios)	1 Core and VideoEncodeScore $\geq$ 4.0
640x360	640x360	2 Cores and VideoEncodeScore $\geq$ 4.5
640x360	1280x720	2 Cores and VideoEncodeScore $\geq$ 4.5
640x360	1920x1080	4 Cores and VideoEncodeScore $\geq$ 4.5
1280x720	1280x720	4 Cores and VideoEncodeScore $\geq$ 7.3
1280x720	1920x1080	4 Cores and VideoEncodeScore $\geq$ 7.3
1920x1080	1920x1080	N/A

### Computer With DXVA But Without Hardware Accelerated Encoder

CAPABLE ENCODER RESOLUTION	CAPABLE DECODER RESOLUTION	REQUIREMENT
424x240	1920x1080	1 Core and VideoEncodeScore $\geq$ 3.0
640x360	1920x1080	2 Cores and VideoEncodeScore $\geq$ 4.5
960x540	1920x1080	2 Cores and VideoEncodeScore $\geq$ 6.0
1280x720	1920x1080	4 Cores and VideoEncodeScore $\geq$ 6.7
1920x1080	1920x1080	4 Cores and VideoEncodeScore $\geq$ 8.2

#### NOTE

The WinSAT score on Windows 7 is limited to a maximum of 7.9. Therefore, the encoding capability for a computer without a hardware accelerated encoder can only be achieved on Windows 8 or Windows 8.1, where the maximum WinSAT score is 9.9.

### Computer With DXVA And With Intel HD Graphics Hardware Accelerated Encoder

CAPABLE ENCODER RESOLUTION	CAPABLE DECODER RESOLUTION	REQUIREMENT
1280x720	1920x1080	All 2nd and 3rd generation Intel HD Graphics
1920x1080	1920x1080	2nd and 3rd generation Intel HD Graphics and GraphicsScore $\geq$ 5.0

## Mobile device video capabilities

The following table describes the maximum video resolutions available on supported mobile devices. For more information about mobile device support, [Mobile client feature comparison for Skype for Business](#).

FEATURE	WINDOWS PHONE	IPHONE	IPAD	ANDROID
H.264 encoding maximum resolution	VGA	QVGA: iPhone 4S VGA: iPhone 5 720p: iPhone 5S and later	VGA: iPad 2 and later/iPad mini 1 and later 720p: iPad Air/iPad mini 2/iPad Pro and later	Up to VGA depending on device model
H.264 decoding maximum resolution	VGA	QVGA: iPhone 4S VGA: iPhone 5 720p: iPhone 5S and later	VGA: iPad 2 and later/iPad mini 1 and later 720p: iPad Air/iPad mini 2/iPad Pro and later	Up to VGA depending on device model



# Plan for Meetings clients (Web App and Meetings App)

5/20/2019 • 9 minutes to read

**Summary:** IT Professionals should review the support requirements for the Skype for Business Web App and Skype Meetings App while planning for Skype for Business Server. This article is not intended for the users of these apps.

Once you've implemented Skype for Business Server, your organization's users will presumably have the Skype for Business client installed as part of the deployment process.

Later on, those users may create meetings and invite users from outside the organization, and those meeting invitees may not have any version of the Skype for Business client. When those users click the URL for the meeting invite, the lack of a client will be detected and the invitee without a Skype for Business client will be asked to download and install a lightweight, meetings-only client so they can join the meeting.

## NOTE

The Skype for Business Web App and Skype Meetings App are only available when trying to log in to a meeting without having Skype for Business. User help for these apps is at <https://aka.ms/smahelp>.

## NOTE

You can't pre-install either the Skype for Business Web App or Skype Meetings App, but [smart phone](#) and [tablet](#) users may be able to install inexpensive mobile clients they can use to attend meetings.

By default, the server hosting the meeting will direct the user to download and install Skype for Business Web App to join the meeting. The Skype for Business Web App is stored on the Front End Server and gets sent to the meeting attendee.

For Skype for Business Server, Skype Meetings App (on Windows) and Skype for Business for Mac (on Mac) are available as replacements for Skype for Business Web App beginning with CU5, but providing the replacement apps requires the additional configuration described in [Enable Skype Meetings App to replace Skype for Business Web App \(Optional\)](#). If Skype Meetings App and Skype for Business for Mac are enabled, users will download the latest version of the apps from the Office 365 Content Delivery Network (CDN) rather than from your Skype for Business server. For Skype for Business Server 2019, using Skype Meetings App and Skype for Business for Mac is the only option.

Skype Meetings App offers a simplified browser experience for downloading and installing the app and joining meetings, including one-click join for users of Internet Explorer. Skype Meetings App also has many improvements over the Skype for Business Web App for reliability and the meeting experience.

## NOTE

As of Skype for Business Server 2015 CU5 or later, meetings held using Skype for Business Online will no longer send a clientless user the Skype for Business Web App, they will instead be sent Skype Meetings App (on Windows) or Skype for Business for Mac (on Mac). As of Skype for Business Server 2015 CU5 or later, if you [Enable Skype Meetings App to replace Skype for Business Web App \(Optional\)](#), clientless users will be sent Skype Meetings App or Skype for Business for Mac instead of Skype for Business Web App.

# Software requirements

To use the Skype for Business Web App, a user must have one of the following supported operating system and browser combinations.

## Operating System and minimum browser support for Skype for Business Web App

OPERATING SYSTEM	EDGE	32- AND 64-BIT INTERNET EXPLORER 11 OR LATER	32- AND 64-BIT INTERNET EXPLORER 10 OR LATER	32- AND 64-BIT INTERNET EXPLORER 9 OR LATER	32- AND 64-BIT VERSION OF SAFARI 6.2.8 - 11.X	32- AND 64-BIT VERSION OF CHROME 18.X OR LATER
Windows 10	Yes	Yes	N/A	N/A	N/A	Yes <b>3</b>
Windows 8.1 <b>1</b>	N/A	Yes	N/A	N/A	N/A	Yes <b>3</b>
Windows 8 (Intel based) <b>1</b>	N/A	N/A	Yes	N/A	N/A	Yes <b>3</b>
Windows 7 with SP1 <b>2</b>	N/A	Yes	No	No	N/A	Yes <b>3</b>
Windows Server 2008 R2 with SP1 <b>2</b>	N/A	Yes	Yes	Yes	N/A	Yes <b>3</b>
macOS 10.8 and later (Intel-based) <b>2</b>	N/A	N/A	N/A	N/A	Yes	Yes

**1** The Skype for Business Web App browser plug-in requires a specific sharing plugin to use computer-based voice, video, sharing, and viewing of ongoing screen sharing and other features. A meeting attendee is given the option to install the sharing plug-in either when they join the meeting or when they initiate one of these features. On Windows 8, and Windows 8.1, the sharing plug-in can be installed only if you're running Internet Explorer 10 or Internet Explorer 11 for the desktop. These features are not available with non-desktop versions of Internet Explorer 10 and 11. Note that Firefox and Safari version 12.0 and later is no longer supported.

**2** On supported Windows 7, Windows Server 2008 R2, and Macintosh operating systems, all features are available including computer-based voice, video, application viewing, application sharing, desktop viewing, and desktop sharing. To use these features, you must install a plug-in when prompted. Note that Mac OS X version 10.7 is no longer supported.

**3** Accessing the Web App from Chrome on Windows will launch a small program which loads the Web App in an embedded Internet Explorer frame. This program requires one of the supported versions of Internet Explorer be installed for the Web App to load properly.

### NOTE

Office 365 users can use Internet Explorer 10 or later with Skype for Business.

## Skype Meetings App

Skype Meetings App runs as an app on computers using Windows 10, Windows 8.1, Windows 8, Windows 7, with 32- and 64-bit Internet Explorer 11 or later installed.

For any other dependencies, refer to [Supported platforms for Skype Meetings App](#)

## Skype for Business for Mac

Skype for Business for Mac runs on computers using macOS version 10.8 or later.

## Hardware requirements

Computer hardware requirements are determined by the operating system and browser. Voice and telephony features require a microphone and speakers, headset with microphone, or equivalent device compatible with the computer. Video features require a video device compatible with the computer. For detailed information about video hardware support and expected video quality, see [Skype for Business client video resolutions](#).

## Network requirements

If a user of Skype for Business Web App or Skype Meetings App experiences meeting connection issues, chances are their organization's network infrastructure is not configured to support Office 365 as described in [Office 365 URLs and IP address ranges](#). This is the case whether the meeting was created by a user of Skype for Business Online or Skype for Business Server.

If the user is on a network not configured as described, many app features may or may not work and they may not be able to connect to the meeting at all.

## Supported Meetings features

This table compares the Meetings features available to users of the Skype for Business client, Skype for Business Web App, Skype Meetings App, and Lync Web App. Lync Web App is listed for feature comparison purposes: a user would only be downloading and using Lync Web App if the meeting was hosted on a Lync 2013 server.

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2016 OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC CLIENT	SKYPE MEETINGS APP	SKYPE FOR BUSINESS WEB APP	LYNC WEB APP
Add computer audio	✓	✓	✓ (requires plug-in)	✓ (requires plug-in)	✓ (requires plug-in)
Add video	✓	✓	✓ (requires plug-in)	✓ (requires plug-in)	✓ (requires plug-in)
Switch audio to a phone for authenticated participants	✓	✓	✓	✓	✓
Switch audio to a phone for guest participants	✓	✓	✓		
View multiparty video (gallery view)	✓	✓	✓	✓	✓
Video-based screen sharing	✓	✓	✓ (View-only)		

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2016 OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC CLIENT	SKYPE MEETINGS APP	SKYPE FOR BUSINESS WEB APP	LYNC WEB APP
Use in-meeting presenter controls	✓	✓	✓	✓	✓
Access detailed meeting roster	✓	✓	✓	✓	✓
Participate in multiparty IM	✓	✓	✓	✓	✓
Set IM messages as high importance	✓				
Share the desktop (if enabled)	✓	✓	✓ (requires plug-in)	✓ (requires plug-in)	✓ (requires plug-in)
Share a program (if enabled)	✓		✓ (On Windows only; requires plug-in)	✓ (On Windows only; requires plug-in)	✓ (On Windows only; requires plug-in)
Take control of another user's shared desktop or program	✓		✓ (1) On Windows only; requires plug-in)	✓ (1) On Windows only; requires plug-in)	✓ (1) On Windows only; requires plug-in)
Let another user take control of your shared desktop or program	✓				
Add anonymous participants (if enabled)	✓	✓	✓	✓	✓
Invite participants by name	✓	✓			
Invite participants by phone number	✓	✓	✓	✓	✓
Invite participants by email	✓		✓	✓	✓
Use dial-in audio meetings	✓ 2	✓ 2	✓ 2	✓ 2	✓ 2
Initiate a Meet Now meeting	✓	✓			

FEATURE/CAPABILITY	SKYPE FOR BUSINESS 2016 OR 2019 CLIENT	SKYPE FOR BUSINESS ON MAC CLIENT	SKYPE MEETINGS APP	SKYPE FOR BUSINESS WEB APP	LYNC WEB APP
Record a meeting	✓				
Add and download attachments	✓		✓	✓	✓
Add and present Microsoft PowerPoint files	✓	✓	✓	✓	✓
Navigate Microsoft PowerPoint files	✓	✓	✓	✓	✓
Add and edit OneNote meeting notes	✓		Edit only (not add)	Edit only (not add)	Edit only (not add)
Use a whiteboard	✓		✓	✓	✓
Conduct polls	✓		✓	✓	✓
Upload files to share with others	✓		✓	✓	✓
Schedule a meeting or conference	Outlook or Skype for Business Web Scheduler	Outlook or Skype for Business Web Scheduler	Skype for Business Web Scheduler	Skype for Business Web Scheduler	Skype for Business Web Scheduler
Q&A Manager	✓		✓	✓	✓
Disable attendee video	✓				
Disable meeting IM	✓		✓	✓	✓
Mute audience	✓	✓	✓	✓	✓
Make everyone an attendee	✓				
Produce Skype Meeting Broadcast	✓				

❶ Participants can't control desktops that are shared by Skype for Business for Mac, Lync for Mac 2011 or Communicator for Mac 2011 users. This also won't work for Skype for Business Web App on Max OSX.

❷ For Skype for Business Online, this feature requires Microsoft PSTN Conferencing, Exchange Unified Messaging, or a 3rd party audio conferencing provider.

3 The Lync for Mac 2011 client cannot view Microsoft Office 2013 PowerPoint presentations when they have been shared in a conference by the Skype for Business Web App.

## Known issues and troubleshooting

For End-users, the [online help](#) for these apps is readily available. IT Professionals should be aware of the following issues:

- If the user is on a network not configured to meet the [Network requirements](#), many app features may or may not work and they may not be able to connect to the meeting at all.
- Some users may have corporate-administered computers with disabled permission to install apps. For those users, neither app is an option, but [smart phone](#) and [tablet](#) users may be able to install inexpensive mobile clients they can use to attend meetings.

Other installation issues are also covered in the [help topics](#).

- Users may see a firewall warning the first time they run the meetings app. They may be prompted to open ports to optimize the experience, and this may require Admin privileges on the machine they may not have. The app should still function and the user can safely decline to open the requested ports.
- You must have [ActiveX enabled without filtering](#) in Internet Explorer, even if IE is not your default browser. In Skype for Business Web App, an ActiveX control—a small module that adds additional features to a web app or other program—is required for audio, video, and screen sharing.
- For some features of Skype for Business Web App to work correctly, you must allow your browser to [save cookies](#) on your computer or device.
- You may need to [turn on JavaScript](#) support in your browser for some Skype for Business Web App features to work as expected.

### AES Support

As of Skype for Business Server 2015 CU5, AES is not supported for ASP.NET 4.6 and this may cause Skype Meetings App to fail to start. [Cryptographic requirements due to ASP .NET 4.5](#) has more details.

## See also

[Deploy Web downloadable clients in Skype for Business Server](#)

[Supported platforms for Skype Meetings App](#)

# Skype Meetings App minimum network requirements

7/18/2019 • 2 minutes to read

**Summary:** Information for organizations who don't use Office 365 and need to access meetings hosted by organizations that do. This article is not intended for the users of these apps.

To allow users to use Skype Meetings App to attend meetings hosted in Skype for Business Online, network administrators of organizations who don't use Office 365 should whitelist or otherwise make available the FQDNs, IPs, and ports mentioned below.

## Requirements for Skype Meetings App connectivity

The information listed here is a subset of [Office 365 URLs and IP address ranges](#), which provides more depth and will always be the most up to date.

APP	DESTINATION FQDNS	IP ADDRESSES	PORTS
<b>Skype Meetings App</b>	*.lync.com *.infra.lync.com *.pipe.aria.microsoft.com *.sfbassets.com *.msecd.net *broadcast.officeapps.live.com *powerpoint.officeapps.live.com *.office.live.com *.cdn.office.net *.s-microsoft.com	These IP addresses are frequently updated. See <a href="#">Skype for Business IP ranges</a> as well as <a href="#">Office IP Ranges</a>	TCP: 80 & 443 UDP: 3478-3481
<b>Teams</b>	*.microsoft.com *.skype.com	These IP addresses are frequently updated. See <a href="#">Skype for Business IP ranges</a> as well as <a href="#">Office IP Ranges</a>	TCP: 443 UDP: 3478-3481

## See also

[Plan for Meetings clients \(Web App and Meetings App\)](#)

[Deploy Web downloadable clients in Skype for Business Server](#)

[Supported platforms for Skype Meetings App](#)

# Plan for Skype for Business in VDI environments

6/25/2019 • 8 minutes to read

This topic discusses planning considerations for using Skype for Business while connecting to a remote virtual desktop.

A Virtual Desktop Infrastructure (VDI) environment is used in some organizations where security and compliance issues are especially sensitive. Their users do their work on a virtual desktop with all their desktop applications and files using Remote Desktop Services or a similar remote connection. Using Skype for Business with full audio and video on a connection like that requires heavy loads of audio and video processing on the client homed on a virtual desktop. Additional VDI plug-in software is available that offloads that processing to the end user's local machine, and reduces the load on the virtual desktop.

There are three solutions available for the VDI plug-in component, offered by Microsoft, Citrix, or VMWare. For new deployments, Microsoft recommends using either the Citrix HDX RealTime Optimization Pack solution or the VMWare Horizon Virtualization Pack. The original Lync VDI Plug-in is still supported for the remainder of its lifecycle.

- The **Lync VDI plug-in** was developed for Lync 2013 and is compatible with either the Lync 2013 or Skype for Business 2015 client running on a virtual desktop. It's a stand-alone application that installs on the local computer and allows the use of local audio and video devices with a client on a virtual desktop. The plug-in does not require a Skype for Business client to be installed on the local computer or thin client, which must run Windows 7, Windows 8, or Windows Server 2008 operating systems. (Thin client devices using these operating systems and supported by Microsoft include: Dell Wyse Z90D7, Dell Wyse R90L7, Dell Wyse X90m7, HP t610 and HP t5740e.) This plug-in is still supported, but no future updates are planned. For Citrix-based virtual environments, the Citrix RealTime Optimization Pack is recommended.
- The **Citrix RealTime Optimization Pack** builds on the Lync VDI plug-in and works with Lync 2013 or Skype for Business 2016 clients on a virtual desktop. It was co-developed by Citrix and Microsoft to improve upon the original VDI Plug-in. It can be installed on clients with Windows and non-Windows operating systems (including Windows 10, Mac and Linux). It consists of two components: the RealTime Connector (which is installed on the virtual desktop) and the RealTime Media Engine (which is installed on the end user's local machine). These two components allow the user's local computer to use the Skype for Business client running on the virtual desktop with the A/V processing moved to the local computer. For Citrix-based virtual desktop environments, the Citrix RealTime Optimization Pack is recommended, and further support is planned.
- The **VMWare Horizon Virtualization Pack** for Skype for Business, developed in collaboration with VMWare, allows you to deliver Skype for Business in a virtual desktop while delivering a great user experience. The solution works by leveraging a media engine at the client to create an optimized solution, with the client endpoint providing media offload capabilities for audio and video calls. This solution that can deliver audio and video either directly between endpoints for one-on-one collaboration, or offload it to a central Multipoint Control Unit (MCU) for multiparty conference calls or meetings.

## NOTE

The Skype for Business Basic clients are not supported with the Citrix HDX RealTime Optimization Pack or the VMWare Horizon Virtualization Pack.

## Citrix HDX RealTime Optimization Pack



Citrix's VDI environment plugin (a feature of XenApp and XenDesktop) is compatible with Lync 2013 and Skype for Business 2015 and 2016 (Full clients using any click to run installer, or MSI installers released after January 2017 PU) clients installed on a virtual desktop. Its overall functioning is based on the Microsoft Lync VDI plug-in, but works on a wider variety of client operating systems, including Windows 10, Macintosh, and Linux.

A full list of features and supported technologies can be found on the Citrix website at [Delivering Microsoft Skype for Business to XenApp and XenDesktop Users](#).

Review the following links for more information:

- Citrix [HDX RealTime Optimization Pack 2.1](#)
- [Technical Overview](#)
- [CTX200279 Skype for Business Feature Support](#)

## VMWare Horizon Virtualization Pack

VMWare's VDI environment solution is compatible with Skype for Business 2015 and 2016 Full clients installed on a virtual desktop. Its overall functioning is based on the Microsoft Lync VDI plug-in, but works on a wider variety of client operating systems, including Windows 10, Macintosh, and Linux.

A full discussion of features and supported technologies can be found on the VMWare website at the following links:

- [What's New in VMware Horizon 7.4 & Horizon Client 4.7](#)
- [Horizon Virtualization Pack for Skype for Business](#)
- [Microsoft Skype for Business With VMware Horizon](#)

## Microsoft's Lync VDI plug-in

With the Microsoft Lync VDI plug-in solution, the user has to be on a Windows computer or thin client and have Microsoft's Lync VDI plugin installed to handle audio/video streams from the client on the virtual desktop. A user will:

1. Connect an audio/video device (like a headset or camera) to a local computer.
2. Connect to a remote virtual desktop with a Lync 2013 or Skype for Business 2015 client.
3. Enter credentials for Skype for Business on the virtual desktop.
4. Re-enter user credentials to establish a connection with the Lync VDI plug-in on the local Windows computer or thin client.

After a connection is established, the user is ready to make and receive audio and video calls. Traffic on the network and the load on the virtual desktop are minimized, since the local computer handles the audio/video processing.

Microsoft's Lync VDI plug-in is only supported on certain Windows operating systems and only supports Lync 2013 or Skype for Business 2015 clients. See [Supported virtualization technologies and known limitations](#) for more details on supported technologies and limitations.

Review the following links for more information:

- [Supported virtualization technologies and known limitations](#)
- [Lync VDI plug-in prerequisites](#)

- [Deploy the Lync VDI plug-in with Skype for Business Server](#)
- Citrix Knowledge Center article [CTX138408](#)

The Microsoft VDI plugin is available at [Microsoft Lync VDI 2013 plugin \(32 bit\)](#) or [Microsoft Lync VDI 2013 plugin \(64 bit\)](#). This plugin is supported with the Skype for Business 2015 client, despite the name.

### Supported virtualization technologies and known limitations

The Lync VDI plug-in allows audio and video calling for supported virtualization technologies. In compliance with standard telephone regulations, support for E911 is also included. The following sections describe the virtualization technologies that are supported by the Lync VDI plug-in and the known feature limitations.

#### Support for Virtualization Technologies

The Lync VDI plug-in supports full desktop remote sessions in the personal virtual desktop scenario, but not in the remote desktop session scenario. These scenarios can be described as follows:

- **Supported: Personalized Virtual Desktops or Virtual Desktop Infrastructure (VDI).** In this scenario, each user logs on to a customizable virtual desktop and is able to save files on the desktop that persist across sessions. Microsoft Remote Desktop Services and VMware Horizon View are example implementations that have been tested for use with Skype for Business 2015. Other implementations undergoing validation include Citrix XenDesktop. For information about vendor-specific VDI environments and client hardware that have been tested by Microsoft, see [Infrastructure qualified for Microsoft Lync](#).
- **Not supported: Remote Desktop Sessions.** In this scenario, each user logs on to a generic virtual desktop session that can't be customized. Examples include Microsoft Remote Desktop Sessions (RDSH) and Citrix XenApp combined with Citrix Receiver.

The Lync VDI plug-in does not support other virtualization technologies, such as application virtualization, which allows the use of an application without requiring installation of the full application locally. Example implementations include Citrix XenApp and Microsoft Application Virtualization (App-V). Application streaming, application remoting, and mixed virtualization modes (for example, application remoting in full desktop remoting) are not supported.

The Lync VDI plug-in was designed to use platform-independent APIs called Dynamic Virtual Channels (DVCs). For scenarios that are not explicitly supported, refer to support statements from the VDI solution provider.

#### Lync VDI plug-in prerequisites

In a VDI environment, the virtual machines and the user's local computer must meet the requirements outlined in this section.

#### NOTE

Your virtualization solution provider can supply details about how to install and deploy their environment. For general information about deploying a virtualized environment based on Hyper-V and Remote Desktop Services, see the following articles in the Microsoft Library: [Hyper-V](#), [Remote Desktop Services in Windows Server 2008 R2](#)

Virtual machines must be configured with Windows 8, Windows 7, or Windows Server 2008 R2 with the latest service packs.

The user's local computer must meet the following requirements:

- The user must be homed on Skype for Business Server or Lync Server 2013.
- The local computer must be running Windows Embedded Standard 7 with SP1, Windows 7 with SP1, or Windows 8.
- If you're using Remote Desktop Services, choose the 32-bit or 64-bit Lync VDI plug-in to match the local

computer's operating system. It's not required for both the local computer and the virtual machine to have 32-bit or 64-bit operating systems. If you're using another virtualization solution or platform, refer to your provider's requirements.

- The local computer must be running the [latest version of the remote desktop client](#). Install the latest updates of Remote Desktop Services client from Microsoft or the latest remote desktop client software from your virtualization solution provider.
- On the local computer, the remote desktop client settings must be configured so that audio plays on the local computer and remote recording is disabled. To configure these settings for Remote Desktop Connection in Windows, see the next section, "To configure Remote Desktop Connection settings."

The Microsoft VDI plugin is available at [Microsoft Lync VDI 2013 plugin \(32 bit\)](#) or [Microsoft Lync VDI 2013 plugin \(64 bit\)](#).

#### **Known Feature Limitations**

The following are known limitations when you use the Skype for Business 2015 client in a VDI environment:

There is limited support for Call Delegation and Response Group Agent Anonymization features.

There is no support for the following features:

- Integrated Audio Device and Video Device tuning pages.
- Multiple-view video.
- Recording of conversations.
- Joining meetings anonymously (that is, joining Skype for Business meetings hosted by an organization that does not federate with your organization).
- Using the Lync VDI plug-in along with a Lync Phone Edition device.
- Call continuity in case of a network outage.
- Customized ringtones and music-on-hold features.

The Lync VDI plug-in is not supported in an Office 365 environment.

#### **NOTE**

The Citrix RealTime Optimization Pack does support Office 365. For Citrix-based virtual environments, review Citrix's [Technical Overview](#) documentation for the list of supported features and versions.

## See also

[Deploy the Lync VDI plug-in with Skype for Business Server](#)

# Plan for high availability and disaster recovery in Skype for Business Server

5/20/2019 • 2 minutes to read

Skype for Business Server offers high availability with server pooling, disaster recovery with pool pairing, and several modes of Back End Server high availability, including AlwaysOn Availability groups, database mirroring, and SQL failover clustering.

High availability refers to making sure that Skype for Business Server services are available even if one or more servers goes down. Disaster recovery refers to keeping services going in the event of a natural or human-caused disaster, and preserving as much data from before the disaster as possible.

As in previous versions of Lync Server, the main high availability feature for most server roles in Skype for Business Server is server redundancy via pooling. If a server running a certain server role fails, the other servers in the pool running the same role take the load of that server. This applies to Front End Servers, Edge Servers, Mediation Servers, and Directors.

Skype for Business Server also provides disaster recovery options for Front End pools. You can set up two pools in different geographical areas to serve as backups for each other. Then if you have an entire pool or site go down, the backup pool can continue to provide service to users at both sites.

Skype for Business Server also supports four modes of high availability for your Back End Servers: SQL mirroring, AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering.

## NOTE

SQL Mirroring is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering methods are preferred with Skype for Business Server 2019.

## NOTE

AlwaysOn Availability Groups are not supported with Persistent Chat Servers.

This section explains these features, and also covers what steps you can take for high availability and disaster recovery for some of your other server roles.

## See also

[Front End Pool high availability and management](#)

[Front End pool disaster recovery in Skype for Business Server](#)

[User experience during pool failure in Skype for Business Server](#)

[Back End Server high availability in Skype for Business Server](#)

[File sharing high availability in Skype for Business Server](#)

# Front End Pool high availability and management

10/9/2019 • 5 minutes to read

Learn about Front End pool management in Skype for Business Server, including managing pools, quorum loss, and special steps for pools with only two Front End Servers.

In Skype for Business Server, the architecture of Front End pools uses a distributed systems model, with each user's data kept on as many as three Front End servers in the pool. We recommend that all your Enterprise Edition Front End pools include at least three Front End Servers.

## Planning for the management of Front End pools

Skype for Business Server uses a distributed systems model based on Windows Fabric. In this model, important data for each user and conference is stored on three Front End Servers in a Front End pool. These three servers storing a certain set of data are called replicas.

With the distributed model for Front End pools, a certain numbers of a pool's servers must be running for the pool to function. There are two loss modes for a pool.

- Routing Group Level quorum loss, caused by not enough replica servers for a particular routing group. A routing group is a set of users homed in the pool. Each routing group has three replicas in the pool: one primary replica and two secondary replicas.
- Pool Level quorum loss, caused when not enough seed servers are running in the pool.

### Routing Group Level quorum loss

The first time you start a new Front End pool, it is essential that 85% of the servers are up and running, as shown in the following table. If fewer servers are running, the services might be stuck in the starting state and the pool might not start.

TOTAL NUMBER OF SERVERS IN THE POOL	NUMBER OF SERVERS THAT MUST BE RUNNING FOR THE POOL TO BE STARTED THE FIRST TIME
2	1
3	3
4	3
5	4
6	5
7	5
8	6
9	7
10	8

TOTAL NUMBER OF SERVERS IN THE POOL	NUMBER OF SERVERS THAT MUST BE RUNNING FOR THE POOL TO BE STARTED THE FIRST TIME
11	9
12	10
16 <b>For Skype for Business Server 2019</b>	12

Every subsequent time the pool is started, 85% of the servers should be started (as shown in the preceding table). If this number of servers cannot be started (but enough servers can be started so that you are not at pool-level quorum loss), you can use the `Reset-CsPoolRegistrarState -ResetType QuorumLossRecovery` cmdlet to enable the pool to recover from this routing group level quorum loss and make progress. For more information about how to use this cmdlet, see [Reset-CsPoolRegistrarState](#).

#### NOTE

In pools with an even number of servers, Skype for Business Server uses the Primary SQL database as Witness. In a pool like this, if you shut down the primary database and switch to the Mirror copy, and shut down enough Front End servers so that not enough are running according to the preceding table, the entire pool will go down. For more information, see [Database Mirroring Witness](#).

#### Pool-level quorum loss

For a Front End pool to function at all, it cannot be in pool-level quorum loss. If the number of servers running falls below the functional level as shown in the following table, the remaining servers in the pool will stop all Skype for Business Server services. Note that the numbers in the following table assume that the Back End Servers in the pool are running.

TOTAL NUMBER OF FRONT END SERVERS IN THE POOL	NUMBER OF SERVERS THAT MUST BE RUNNING FOR POOL TO BE FUNCTIONAL
2	1
3-4	Any 2
5-6	Any 3
7	Any 4
8-9	Any 4 of the first 7 servers
10-12	Any 5 of the first 9 servers
12-16 <b>For Skype for Business Server 2019</b>	Any 7 of the first 12 servers

In the preceding table, the "first servers" are the servers which were brought up first, chronologically, when the pool was started for the first time. To determine these servers, you can use the `Get-CsComputer` cmdlet with the `-PoolFqdn` option. This cmdlet will show the servers in the order that they appear in the topology, and the ones at the top of the list are the first servers.

#### IMPORTANT

The maximum number of front end servers has been increased to 16 in [Skype for Business Server 2019](#)

### Additional steps to ensure pools are functional

You should watch for a couple of other factors to ensure that your Front End pools remain functional.

- When you move users to the pool for the first time, be sure at least three of the Front End Servers are running.
- If you establish a pairing relationship between this pool and another pool for disaster recovery purposes, then after establishing that relationship you must be sure this pool has three Front End servers running simultaneously at some time to properly synchronize data with the backup pool. For more information on pool pairing and disaster recovery features, see [Plan for high availability and disaster recovery in Skype for Business Server](#).

## Front End pool with two Front End servers

We do not recommend deploying a Front End pool that contains only two Front End Servers. This small pool will not provide a robust high-availability solution like a larger pool would, and needs extra care in managing. Additionally, if the Back End Server of a two-server pool went down, the whole pool itself would likely soon go down as well. If you want to deploy just one or two servers running Skype for Business Server, we recommend you deploy them as Standard Edition servers.

If you do ever need to deploy a pool with two Front End Servers, follow these guidelines:

- If one of the two Front End Servers goes down, you should try to bring the failed server back up as soon as you can. Similarly, if you need to upgrade one of the two servers, bring it back online as soon as the upgrade is finished.
- If for some reason you need to bring both servers down at the same time, do the following when the downtime for the pool is finished:
  - The best practice is to restart both Front End Servers at the same time.
  - If the two servers cannot be restarted at the same time, you should bring them back up in the reverse order of the order they went down.
  - If you cannot bring them back up in that order, then use the following cmdlet before bringing the pool back up: `Reset-CsPoolRegistrarState -ResetType QuorumLossRecovery -PoolFQDN <FQDN>`

## Front End pool configuration failures and changes

If a Front End server fails and is unlikely to be replaced for a few days or more, remove the server from the topology. Add the new Front End server to the topology when it is available again.

Whenever you make a configuration change to a Front End pool, such as adding or removing servers, you must follow these guidelines:

- After the new topology has been published, you must restart each Front End server in the pool. Restart them one at a time.
- If the entire pool has been down during the configuration change, then run the following cmdlet after the new topology is published: `Reset-CsPoolRegistrarState -PoolFQDN <PoolFQDN> -ResetType ServiceReset`

# Front End pool disaster recovery in Skype for Business Server

10/1/2019 • 7 minutes to read

For disaster recovery, Skype for Business Server offers pool pairing with failover in case one pool goes down.

For the most robust disaster recovery options in Skype for Business Server, deploy pairs of Front End pools across two geographically dispersed sites. Each site has a Front End pool which is paired with a corresponding Front End pool in the other site. Both sites are active, and the Backup Service provides real-time data replication to keep the pools synchronized. See [Deploy paired Front End pools for disaster recovery in Skype for Business Server](#) if you want to implement Front End pool pairing.



If the pool in one site fails, you can fail over the users from that pool to the pool in the other site, which then serves all the users in both pools. For capacity planning, you should design each pool to be able to handle the workload of all users in both pools in the event of a disaster.

Two data centers that include Front End pools paired with each other can be any distance apart. We recommend that you pair two data centers in the same world region, with high-speed links between them.

Having two data centers across world regions is possible, but could incur higher data loss if there is a disaster, because of latency in data replication.

When you plan which pools to pair, you must keep in mind that only the following pairings are supported:

- Enterprise Edition pools can be paired only with other Enterprise Edition pools. Similarly, Standard Edition pools can be paired only with other Standard Edition pools.
- Physical pools can be paired only with other physical pools. Similarly, virtual pools can be paired only with other virtual pools.
- Pools that are paired together must be running the same base operating system.

Neither Topology Builder nor topology validation will prohibit pairing two pools in a way that does not follow these recommendations. For example, Topology Builder allows you to pair an Enterprise Edition pool with a Standard Edition pool. However, these types of pairings are not supported.

## Backup Registrar relationships and Survivable Branch Appliances

In addition to providing disaster recovery ability, two paired pools serve as the backup Registrars for each other. Each pool can be the backup for only one other Front End pool.

Even though backup relationships between two Front End pools must be 1:1 and symmetrical, each Front End pool



can still also be the backup registrar for any number of Survivable Branch Appliances.

Note that Skype for Business does not extend disaster recovery support to users homed on a Survivable Branch Appliance. If a Front End pool that serves as the backup for a Survivable Branch Appliance goes down, users signed into the Survivable Branch Appliance fall into resiliency mode even though users homed on the Front End pool are failed over to the backup Front End pool.

## Recovery time for pool failover and pool failback

For pool failover and pool failback, the engineering target for recovery time objective (RTO) is 15-20 minutes. This is the time required for the failover to happen, after administrators have determined there was a disaster and started the failover procedures. It does not include the time for administrators to assess the situation and make a decision, nor does it include the time for users to sign in again after failover is complete.

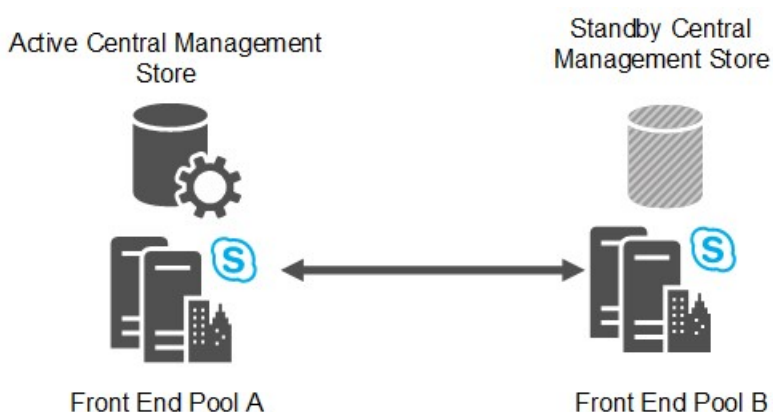
For pool failover and pool failback, the engineering target for recovery point objective (RPO) is 5 minutes. This represents the time measure of data that could be lost due to the disaster, due to replication latency of the Backup Service. For example, if a pool goes down at 10:00 A.M., and the RPO is 5 minutes, data written to the pool between 9:55 A.M. and 10:00 A.M. might not have replicated to the backup pool, and would be lost.

All RTO and RPO numbers in this document assume that the two data centers are located within the same world region with high-speed, low-latency transport between the two sites. These numbers are measured for a pool with 40,000 concurrently active users and 200,000 users enabled for Skype for Business with respect to a pre-defined user model where there is no backlog in data replication. They are subject to change based on performance testing and validation.

## Central Management store failover

The Central Management store contains configuration data about the servers and services in your deployment. Each Skype for Business Server deployment includes one Central Management store, which is hosted by the Back End Server of one Front End pool.

If you pair the pool that hosts the Central Management store, a backup Central Management store database is set up in the backup pool. At any point, one of the two Central Management store databases is active, and the other is a standby. The content is replicated by the Backup Service from the active database to the standby.



During a pool failover that involves the pool hosting the Central Management store, you must fail over the Central Management store before you fail over the Front End pool.

After the disaster is repaired, it is not necessary to fail back the Central Management store. The Central Management store can remain in the pool you failed it over to.

The engineering targets for Central Management store failover are 5 minutes for recovery time objective (RTO) and 5 minutes for recovery point objective (RPO).

# Front End pool pairing data security

The Backup Service transfers user data and conference content between two paired Front End pools continuously. The user data contains user SIP URIs as well as conference schedules, contact lists and settings. Conference content includes Microsoft PowerPoint uploads, as well as whiteboards used in conferences.

From the source pool, this data is exported from the local storage, zipped, and then transferred to the target Pool, where it is unzipped and imported to local storage. The Backup Service assumes that the communications link between the two data centers is within the corporate network that is protected from the Internet. It does not encrypt the transferred data between the two data centers, nor is the data natively encapsulated within a secure protocol, such as HTTPS. Therefore, a man-in-the-middle attack from internal personnel within the corporate network is possible.

Any enterprise which deploys Skype for Business Server across multiple data centers and uses the disaster recovery feature must ensure that traffic between data centers is protected by their corporate Intranet. Enterprises that care about internal attack protection must secure the communication links among the data centers. This is a standard requirement that also helps protect many other types of corporate sensitive data transferred among data centers.

While the risk of man-in-the-middle attacks within the corporate network exists, it is relatively contained as compared to exposing the traffic to the Internet. Specifically, the user data exposed by Backup Service (such as SIP URIs) are generally available to all employees within the company via other means such as the Global Address Book or other directory software. Hence, your focus should be on securing the WAN between the two data centers when the Backup Service is used to copy data between the two paired pools.

## Mitigating security risks

You have many ways to enhance security protection for the Backup Service traffic. This ranges from restricting access to the data centers to securing the WAN transport between the two data centers. In most cases, enterprises deploying Skype for Business Server might already have the required security infrastructure in place. For enterprises looking for guidance, Microsoft provides a solution as an example of how to build a secure IT infrastructure. For details, see <https://go.microsoft.com/fwlink/p/?LinkId=268544>.

We do not imply that it is the only solution, nor do we imply that it is the preferred solution for Skype for Business Server. We recommend that enterprise customers choose the solution suits their specific needs, based on their IT security infrastructure and requirements. The example Microsoft solution employs IPSec and Group Policy for Server and Domain Isolation.

Another possible solution is to use IPSec just to help secure the data sent by the Backup Service itself. If you choose this method, you should configure the IPSec rules for the SMB protocol for the following servers, where Pool A and Pool B are two paired Front End pools.

- The SMB Service (TCP/445) from each Front End Server in Pool A to the File Store used by Pool B.
- The SMB Service (TCP/445) from each Front End Server in Pool B to the File Store used by Pool A.

### Caution

IPsec is not intended as a replacement for application-level security, such as SSL/TLS. One advantage of using IPsec is that it can provide network traffic security for existing applications without having to change them. Enterprises that want to just secure the transport between the two data centers should consult their respective networking hardware vendors about ways to set up secure WAN connections by using the vendor's equipment.

## See also

[Deploy paired Front End pools for disaster recovery in Skype for Business Server](#)

# User experience during pool failure in Skype for Business Server

5/20/2019 • 4 minutes to read

Learn about what users experience when a Front End pool fails over or fails back during disaster recovery in Skype for Business Server.

If a pool is failed over, all users in the affected pool are forced to sign out and then sign into the backup pool. For a brief period users who sign into the backup pool may be in resiliency mode. In Resiliency mode, users are unable to perform tasks that would cause a persistent change on Skype for Business Server, such as adding a contact. After the failover is complete, all users can get all services from the backup pool.

Any calls, meetings, or conversations a user has when the pool fails are disrupted, and the user must re-establish those sessions after failover to continue.

Users are not rehomed during failover or failback. Users who are homed on a pool that fails will be temporarily serviced by the backup pool. When the home pool is restored, the administrator can fail back these users to be serviced by their original pool, where they are still homed.

Note that the Location Information Server database is not replicated to the backup pool. For best practice, the administrator should regularly back up the LIS database and use the latest backup copy to restore the LIS database in the backup pool after the failover.

## User experience during failover

When a user is in a pool that fails, the user is logged out. Any peer-to-peer session the user was participating in is ended, as are conferences organized by that user. The user cannot log back in until either the registrar resiliency timer expires or the administrator initiates failover procedures, whichever comes first. When the user logs back in, they will log in to the backup pool. If they log in before the failover has completed, they will be in Resiliency mode until failover is complete. Only then can a user establish new sessions or re-establish previous sessions.

## User experience during failback

Pool failback can happen while an affected user is logged on to the backup pool, and the user remains logged on and working during the failback. Note that the failback process takes several minutes to complete. For reference, it is expected to take up to 60 minutes for a pool of 20,000 users.

The following tables show more details about how a user is affected during and after failback, and also how users in other pools see and interact with a user in a pool who is being failed back.

The term affected user refers to any user who was failed over from the home pool and is being serviced by the backup pool. A user originally homed on the backup pool is not an affected user.

### User Experience for an Affected User in a Pool in Failback

USER STATE OR TASK	DURING FAILBACK	AFTER FAILBACK COMPLETION
User state of user already logged in	User stays signed in and connected to backup pool. At some point user will be signed out and sign back in to the original home pool, in Resiliency mode.	User remains signed in and goes into regular mode.

<b>USER STATE OR TASK</b>	<b>DURING FAILBACK</b>	<b>AFTER FAILBACK COMPLETION</b>
New user logging in	User can sign in to the home pool in Resiliency mode.	User can sign in to the original home pool in regular mode.
Ongoing conferences organized by affected user	All modalities of conference are terminated. Rejoin button will appear, but no users can rejoin while the affected user is in Resiliency mode.	All modalities now work. Every participant needs to click to rejoin the conference.
Ongoing conferences organized by unaffected user	Conference continues and affected user can stay in the conference. Affected user is restricted to what he/she can do in Resiliency mode.	Conference continues, and affected user can stay in the conference and all modalities work after user exits Resiliency mode.
Scheduling or modifying scheduled meetings, creating ad-hoc conferences	Not possible while user is in Resiliency mode.	Available for all modalities.
Presence as seen by other users in the same pool	Presence unknown while user is signed into backup pool during Resiliency mode.	Shows the last presence state set by the user, and presence changes will now be reflected.
Contacts list and Address Book Service availability	Not available	Available
All peer-to-peer sessions and modalities	Available	Available

### **User Experience for a User Homed in an Unaffected Pool During Failback of Another Pool**

<b>USER TASK</b>	<b>DURING FAILBACK</b>	<b>AFTER FAILBACK COMPLETION</b>
Viewing presence of affected user	Shows the last presence state set by the affected user.	Working. Unaffected users see updates made by affected users.
Ongoing conferences organized by affected user	All modalities of conference are terminated.	All modalities now work. Every participant needs to click to rejoin the conference.
Ongoing conferences organized by unaffected user	Conference continues, and affected user can stay in the conference and all modalities work.	Conference continues, and affected user can stay in the conference and all modalities work.
All peer-to-peer sessions and modalities	Available	Available

# Back End Server high availability in Skype for Business Server

5/20/2019 • 7 minutes to read

Learn about the Back End Server high availability options supported in Skype for Business Server, including AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances, database mirroring, and SQL failover clustering.

To enhance high availability for your Back End Servers, you have four options:

- Database mirroring
- AlwaysOn Availability Groups
- AlwaysOn Failover Cluster Instances (FCI)
- SQL failover clustering

Using one of these solutions is optional, but is recommended to maintain your organization's business continuity. Otherwise, having a single database server go down could cause the loss of significant Skype for Business Server data.

You can set up database mirroring using only Topology Builder. For AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances, or SQL failover clustering, you use SQL Server to create the high availability solution, then you can use Topology Builder to associate it with a Front End pool.

If you use Back End Server high availability on a Front End pool that is paired with another Front End pool for disaster recovery, you should use the same Back End high availability solution in both pools.

## Database mirroring

Skype for Business Server supports mirroring with the following database software:

- SQL Server 2017, both Enterprise Edition and Standard Edition
- SQL Server 2016, both Enterprise Edition and Standard Edition
- SQL Server 2014, both Enterprise Edition and Standard Edition
- SQL Server 2012 SP2 and CU2, both Enterprise Edition and Standard Edition

### NOTE

SQL Mirroring is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering methods are preferred with Skype for Business Server 2019.

Asynchronous database mirroring is not supported for Back End Server high availability in Skype for Business Server. In the rest of this document, database mirroring means synchronous database mirroring, unless otherwise explicitly stated.

When you deploy database mirroring in a Front End pool, all Skype for Business Server databases in the pool are mirrored, including the Central Management store, if it is located in this pool, as well as the Response Group

application database and the Call Park application database, if those applications are running in the pool.

With database mirroring, you do not need to use shared storage for the servers. Each server keeps its copy of the databases in local storage.

You may choose to deploy database mirroring with or without a witness. We recommend using a witness because it enables failover of the Back End Server to be automatic. Otherwise, an administrator must manually invoke failover. Note that even if a witness is deployed, an administrator can manually invoke Back End Server failover, if necessary.

If you use a witness, you can use a single witness for multiple pairs of Back End Servers. There is no strict 1:1 correspondence between witnesses and pairs of Back End Servers. Deployments that use a single witness for multiple pairs of Back End Servers are not quite as resilient as topologies with a separate witness for each Back End Server pair.

### Guidelines for planning Back End Server mirroring

In general, setting up SQL mirroring between the two Back End Servers with a witness requires the following:

- The primary server's version of SQL Server must support SQL mirroring.
- The primary, mirror, and the witness (if deployed) must have the same version of SQL Server.
- The primary and the mirror must have the same edition of SQL Server. The witness may have a different edition.

For SQL best practices in terms of what SQL versions are supported for a Witness role, see "[Database Mirroring Witness](#)" in the MSDN Library.

Before configuring server mirroring, you must first set up SQL database permissions correctly. For details, see "[Set Up Login Accounts for Database Mirroring or AlwaysOn Availability Groups \(SQL Server\)](#)".

With SQL mirroring, database recovery mode is always set to **Full**, which means you must closely monitor transaction log size and back up transaction logs on a regular basis to avoid running out of disk space on the Back End Servers. The frequency of transaction log backups depends on the log growth rate, which in turn depends on database transactions incurred by user activities on the Front End pool. We recommend that you determine how much transaction log growth is expected for your Lync deployment workload so that you can do the planning accordingly. The following articles provide additional information on SQL backup and log management:

#### IMPORTANT

Using Topology Builder or cmdlets to set up and remove SQL mirroring is supported only when the primary, mirror, and witness (if desired) servers all belong to the same domain. If you want to set up SQL mirroring among servers in different domains, see your SQL Server documentation.

#### NOTE

SQL Mirroring is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering methods are preferred with Skype for Business Server 2019.

### Recovery time for automatic Back End Server failover with database mirroring

For automatic Back End failover with database mirroring, the engineering target for recovery time objective (RTO) is 5 minutes. Because of the synchronous database mirroring, we do not anticipate data loss during Back End Server failures except in rare occasions when both the Front End Servers and the Back End Server go down simultaneously while data is being moved between the servers. The engineering target for recovery point objective (RPO) is 5 minutes.

## User experience during Back End Server failure with database mirroring

User experience during a failure depends on the nature of the failure, and on your topology.

If you use database mirroring and have a witness configured, and the principal fails, Back End Server failover happens automatically and quickly. Active users should not notice much interruption to their ongoing sessions.

If there is no witness configured, it will take some time for the administrator to manually invoke the failover. During that time, active users may be affected. They will continue their sessions as normal for about 30 minutes. If the primary is still not restored, or an administrator has not failed over to the backup, then users are switched to Resiliency mode, meaning that they are unable to perform tasks that require a persistent change on Lync Server (such as adding a contact).

If both the principal and the mirror Back End Servers fail, or if one of those servers and the witness fails, the Back End Server will become unavailable (even if it is the principal that is still working). In this case, active users are switched to Resiliency mode after some time.

## AlwaysOn Availability Groups and AlwaysOn Failover Cluster Instances

Skype for Business Server supports AlwaysOn Availability Groups only as active/passive, not active/active.

To use AlwaysOn Availability Groups or AlwaysOn Failover Cluster Instances, you first use SQL Server to set up and configure the high availability solution. You can then use Topology Builder to associate it with a Front End pool.

Skype for Business Server supports AlwaysOn with the following database software:

- SQL Server 2017 Enterprise Edition
- SQL Server 2017 Standard Edition with limitations, see note below
- SQL Server 2016 Enterprise Edition
- SQL Server 2016 Standard Edition with limitations, see note below
- SQL Server 2014 Enterprise Edition
- SQL Server 2012 SP2 and CU2 Enterprise Edition

### NOTE

SQL Server 2017 and SQL Server 2016 are the only versions supported by Skype for Business Server 2019.

### NOTE

Always On Availability Groups is **not** supported in SQL 2016 and 2017 Standard Editions but you can use Always On Failover Cluster Instances. See [Editions and supported features of SQL Server 2016](#) to learn more.

### IMPORTANT

Instance names for multiple AlwaysOn Availability Group instances must be the same.

For steps for deploying AlwaysOn Availability Groups, see [Deploy an AlwaysOn Availability Group on a Back End Server in Skype for Business Server](#).

# SQL Server Failover Clustering

Skype for Business Server supports SQL Server failover clustering with the following database software:

- SQL Server 2017, both Enterprise Edition and Standard Edition
- SQL Server 2016, both Enterprise Edition and Standard Edition
- SQL Server 2014, both Enterprise Edition and Standard Edition
- SQL Server 2012 SP2 and CU2, both Enterprise Edition and Standard Edition

To use SQL failover clustering, you should first set up and configure the SQL Server cluster before deploying your Front End pool. For best practices and setup instructions for failover clustering in SQL Server 2012, see <https://technet.microsoft.com/en-us/library/hh231721.aspx>.

## **NOTE**

SQL Server 2017 and SQL Server 2016 are the only versions supported by Skype for Business Server 2019.

To use SQL failover clustering, you should first set up and configure the SQL Server cluster before deploying your Front End pool. For best practices and setup instructions for failover clustering in SQL Server 2014 and 2016, see <https://technet.microsoft.com/en-us/library/hh231721.aspx>. For failover clustering in SQL Server 2008, see [https://technet.microsoft.com/en-us/library/ms189134\(v=sql.105\).aspx](https://technet.microsoft.com/en-us/library/ms189134(v=sql.105).aspx).

When you install SQL Server, you should install SQL Server Management Studio to manage the locations for database and log file locations. SQL Server Management Studio is installed as an optional component when you install SQL Server.



# File sharing high availability in Skype for Business Server

5/20/2019 • 2 minutes to read

Learn about ensuring high availability of your file shares in Skype for Business Server, using DFS.

To ensure high availability for file sharing in your Skype for Business Server deployment, you can use the Distributed File System (DFS). DFS supports failover from one file server to another within the same data center. For a large scale deployment, we recommend that you use dedicated file servers that are paired using DFS. For more information on DFS in Windows Server 2012, see <https://go.microsoft.com/fwlink/?LinkId=524384>. For information on DFS on Windows Server 2008, see <https://go.microsoft.com/fwlink/p/?LinkId=524385>.

Depending on your network's size, and the amount of resiliency you want, you can use one pair of servers to host all file shares in a site, or use one pair per Front End pool.

DFS is a best effort file replication mechanism, with no published recovery time objective (RTO) or recovery point objective (RPO) commitment. A failover between DFS servers should be completed quickly, but data replication delay may prevent users from being able to continue work in progress when the failover happens.

If you use DFS and the data store on the fileshare is critical, you should back up the file shares frequently, such as every 4 to 8 hours. When one file share goes down and replication is not up to date, you can use the backup to restore the content on the failed server to the other server that is paired with the server that is now unavailable.

# Plan for instant messaging and presence in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn how to plan for instant messaging and presence in Skype for Business Server.

Plan for instant messaging and presence in Skype for Business Server. To learn about specific deployment options, such as enabling or disabling Offline Instant Messaging (IM), see [Deploy instant messaging and presence in Skype for Business Server](#).

## Plan for instant messaging and presence in Skype for Business Server

Front End Servers provide core Skype for Business Server functionality such as instant messaging (IM) and presence and are included in every Skype for Business Server deployment. There are two editions available: Skype for Business Server Enterprise Edition, which is designed primarily for larger organizations, and Skype for Business Server Standard Edition, which is designed primarily for smaller organizations which want a smaller hardware investment and do not require full high availability options. Both editions support all Skype for Business Server workloads including IM, presence, conferencing, and Enterprise Voice.

Instant messaging (IM) enables your users to communicate with each other in real time on their computers using text-based messages. Both two-party and multiparty IM sessions are supported. A participant in a two-party IM conversation can add a third participant to the conversation at any time. When this happens, the Conversation window changes to support conferencing features.

Presence provides information to users about the status of others on the network. A user's presence status provides information to help others decide whether they should try to contact the user and whether to use instant messaging, phone, or email. Presence encourages instant communication when possible, but it also provides information about whether a user is in a meeting or out of the office, indicating that instant communication is not possible. This presence status is displayed as a presence icon in Skype for Business and other presence-aware applications, including the Microsoft Outlook messaging and collaboration client, Microsoft SharePoint technologies, and Microsoft Office. The presence icon represents the user's current availability and willingness to communicate.

### Technical requirements

Instant messaging (IM) and presence always run on Enterprise Edition Front End pools and Standard Edition servers. For information on supported hardware, operating systems, and database software, see [Certified Gateways, Requirements for your Skype for Business 2015 environment](#), and [Infrastructure requirements for Skype for Business Server 2019](#).

### Enabling communication with external users

You can greatly increase the benefits of your investment in Skype for Business Server by enabling your users to communicate with external users. External users can include:

- Remote users: Your organization's own users, when they are working outside your firewalls and are using their laptops or other Skype for Business Server devices.
- Federated users: Users from companies you work with who also run Skype for Business Server. To enable your users to easily contact these users, you create federated relationships with these companies.
- Skype users: Skype for Business users can reach the hundreds of millions of users on Skype with IM, voice and video.

**NOTE**

AOL, Yahoo, and Google Talk are no longer supported.

**NOTE**

To enable any or all of these scenarios, you need to deploy an Edge Server to help enable secure communications between your Skype for Business Server deployment and external users. Your organization's remote users and users at federated organizations will be able to see each other's presence and communicate using IM.

**NOTE**

Extensible Messaging and Presence Protocol (XMPP) is only supported for Unified Capabilities Collaboration Platform (UCCP) Joint Interoperability Test Command (JITC) certification scenarios.

**Archiving IM content**

Skype for Business Server provides features you can use if your organization must follow compliance regulations. You can use Archiving to archive the content of IM messages for all users in your organization or for only certain users that you specify. For details, see [Plan for archiving in Skype for Business Server](#).

If you also have Microsoft Exchange Server 2013 deployed, you can integrate the archiving of Exchange data with the archiving of Skype for Business Server data, and use a single tool to search both types of archived data. For more information, see [Configure Skype for Business Server to use Exchange Server archiving](#).

**Topologies and components**

The only components required for instant messaging (IM) and presence are:

- Your organization's Front End servers (known as a pool) or a Standard Edition server. IM and presence capabilities are always enabled on these servers. For more information on Front End pool topologies and management, see [Front End Pool high availability and management](#).
- A load balancer, if you have an Enterprise Edition Front End pool.

**Supported collocation**

Collocation is defined as having a single server, or group of servers, with multiple roles installed. For details on collocation, see [Topology Basics for Skype for Business Server](#).

# Plan for Video Interop Server in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Review this topic while planning to integrate Skype for Business Server with third-party teleconferencing devices.

Skype for Business Server now allows you to integrate with certain third-party VTC (Video Teleconferencing System) solutions. The new server role that enables this video conferencing interoperability is the Video Interop Server (VIS), which is currently implemented as a standalone server role available only for on-premises installations. A VIS acts as an intermediary between a third party teleconference system and a Skype for Business Server deployment. For this release, VIS is focused on interoperability with Cisco/Tandberg video systems. Review this article to determine whether to use this feature in your Skype for Business Server installation.

## Device interoperability

Interoperation is tested and supported with Cisco VTCs registering with Cisco Unified Communications Manager (CallManager, or CUCM) version 10.5 and TCP SIP trunks set up between CUCM and the VIS.

The currently supported VTCs are:

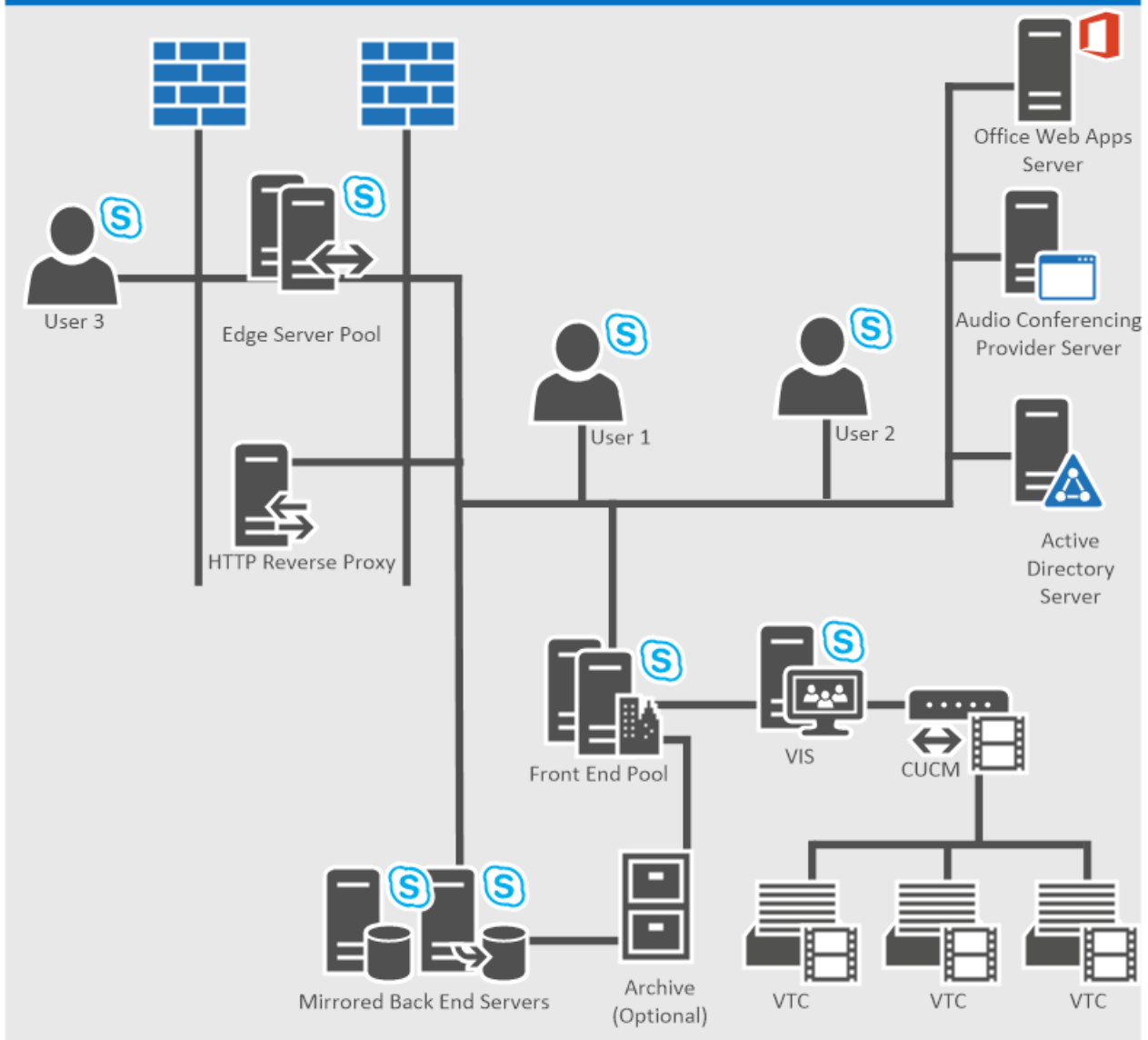
- Cisco C40
- Cisco C60
- Cisco C90
- Cisco MX200
- Cisco MX300
- Cisco DX80
- Cisco EX60
- Cisco EX90
- Cisco SX20

### NOTE

Cisco software release TC7.0.0 or above is required on these systems for integration with Skype for Business Server to work as expected.

## SIP trunks

The Video Interop Server functions in SIP trunk mode, where the VTCs continue to register with the existing Cisco infrastructure - for example, Cisco Call Manager (CUCM). A video SIP trunk is defined between CUCM and the VIS so that calls can be routed between the two systems. Only calls over the SIP trunk from the VTC to the VIS are supported. Thus, VTCs can dial into a Skype for Business conference (by dialing the phone number associated with the Call Automated Attendant), but cannot be dragged and dropped into the conference.



## Features

This server role provides:

- Conversion between the H.264 formats used by 3rd party video systems and the Skype for Business Server deployment.
- Conversion of a single video stream at a given resolution from a VTC into multiple simulcast streams of different resolutions for use in the Skype for Business Server deployment. These streams can be sent to the AVMCU and then to Skype for Business Server endpoints and other video systems that have requested different resolutions. This conversion is also used when the third party video system is involved in a Skype for Business A/V conference call. Once the transcoding limit is reached in a particular VIS server, any following requests for different resolutions will only receive a stream with the lowest resolution.
- Support for a video SIP trunk between the CUCM gateway and a Skype for Business Server Video Interop Server; VTCs continue to register with the Cisco gateway, and initiate calls to the Skype for Business deployment through the gateway. Calls are routed from the gateway to the Skype for Business Video Interop Server over the video SIP trunk.
- Support for a user in a conference room with a supported video system to dial from that system to join an open or closed conference. This call will traverse the video SIP trunk.

- Support for a user in a conference room with a supported video system to call a Skype for Business client. The call will traverse the SIP trunk.
- Support for mid-call control from the Skype for Business Server side or from the supported VTC system for both point to point and multipoint calls including mute/un-mute audio, pause/resume video, lock video, and hold/un-hold call.

## Known limitations

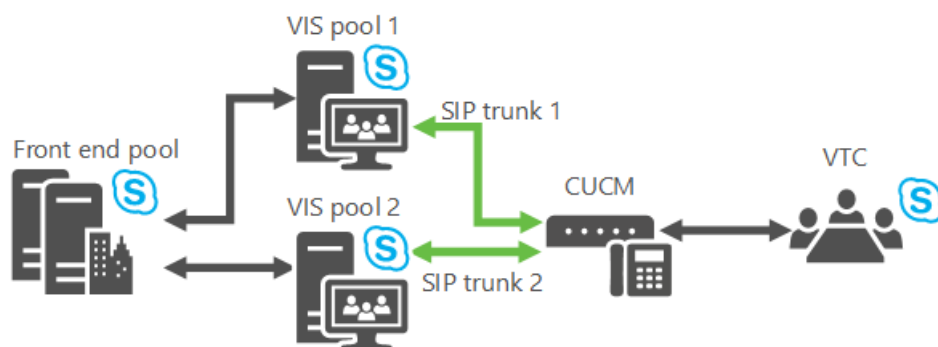
This server role has the following limitations:

- New calls from the Skype for Business deployment to the VTCs over the video SIP trunk are not supported. . This means that only new calls from the VTCs into the Skype for Business deployment are supported over the video SIP trunk. Presence for the supported video system will not be available over the video SIP trunk to the VIS.
- Only a standalone VIS pool will be supported for video SIP trunk mode.
- TLS + SRTP or TCP + RTP will be supported for communications between the VTC and VIS over the video SIP trunk.
- Application sharing is not supported. A Skype for Business user in the conference room needs to join the Skype for Business conference (via a laptop for example) and display the app sharing screens on one of the free monitors in the conference room not associated with the VTC.
- The ability for a VTC to join a federated meeting via VIS is not supported.
- The ability for a VTC to join an online meeting via VIS is not supported.
- Calls from a VTC to the PSTN via VIS are not supported.
- Calls from the PSTN to a VTC via VIS are not supported.

## Resiliency mechanisms

The VIS supports incoming calls from a CUCM that are carried over a video SIP trunk. It's possible to lose connectivity either upstream or downstream, so for robust resiliency consider both possibilities:

1. **VIS Pool Failover** If the main VIS pool that the video gateway points to is down, recovery is possible if the video gateway has defined trunks to two (or more) VIS pools. If the video gateway determines it cannot make calls to the primary VIS pool, it simply routes the calls to a secondary VIS pool.



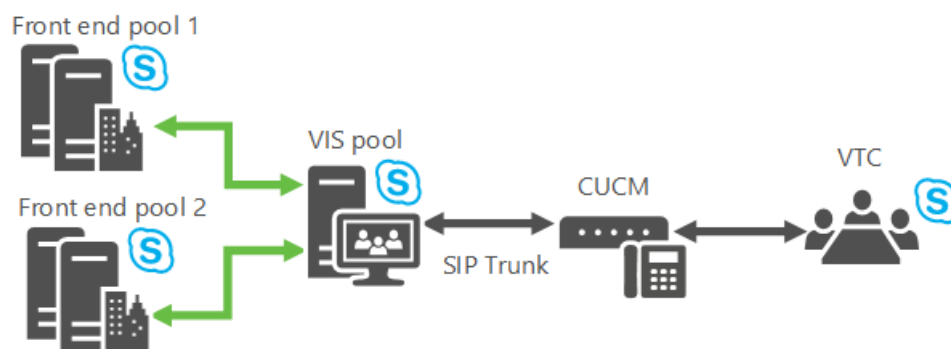
A particular VIS pool can have trunks to multiple gateways, but normally a particular gateway can't have trunks to multiple VIS pools, so a trick needs to be done to support this failover: Define 2 FDQNs in DNS which resolve to the same IP address of a video gateway. Represent each FQDN as a separate video gateway in the Topology Document where each video gateway has a trunk to a different VIS pool, and recovery is now possible. (If TLS is used, the multiple names will need to be in the SAN of the video

gateway certificate.)

#### NOTE

VIS only allows incoming calls from gateways configured in the Topology Document.

2. **Front End failover** If a VIS pool receives a call from CUCM but cannot reach its primary next-hop Registrar or Front End pool, calls are routed to a backup Front End pool.



The VIS will keep track of the status of its primary Front End pool and its backup Front End pool (the setting is found in the backup setting for the Registrar service in the Topology Document). It sends Options polls once a minute to both pools, and if there are five consecutive failures the VIS assumes that a particular Front End pool is down. If the primary Front End pool is marked as down and there is an available configured backup the VIS sends new calls from the gateway to the backup Front End pool. Once the primary Front End pool comes back, the VIS will resume using the primary Front End pool for new calls.

The VIS will also implement a 10 second timer for calls from the video SIP trunk. If the primary next-hop Front End pool was used for a call from the video SIP trunk, and the primary next-hop Front End pool did not answer with some SIP message (including 100 Trying) to the Invite sent to it within this timer value, the backup next-hop proxy for the call should be tried if configured.

#### NOTE

If the backup next hop was tried first, the primary will not be tried next.

The admin could also use the Windows PowerShell failover command to force VIS to use the backup Front End pool, for example, when maintenance has to be performed on the primary Front End pool.

## Co-existence of Voice and Video Trunks to the Same Gateway Peer

Skype for Business Server supports having voice and video SIP trunks use the same gateway peer. So the same CUCM deployment could have voice SIP trunks to the Mediation Server and video SIP trunks to VIS.

- A PSTN Gateway will need to be defined with a particular FQDN in the Topology Document for the voice SIP trunks.
- The peer to the PSTN Gateway will be the Mediation Server.
- Multiple voice trunks can be defined spanning from a PSTN Gateway to multiple Mediation Server pools if necessary.
- A Video Gateway will need to be defined in the Topology Document for the video SIP trunk with the same FQDN as for the PSTN Gateway.
- The peer to the Video Gateway will be VIS.

- A single video trunk can be defined from a Video Gateway to a particular VIS pool.
- CUCM will need to be configured to correctly route calls over the voice trunk vs. the video trunk. For example, a special dial prefix could be used when dialing from the VTC; CUCM could associate this dial prefix with calls to VIS, and appropriate translation rules would strip this prefix from the SIP Invite to VIS.

## Co-existence of VIS in the Skype for Business Release with Previous Releases of Lync

VIS can only be deployed as part of Skype for Business deployment. It can interoperate with Lync 2013 conferences and clients that are a part of an existing deployment; in those cases, the VIS pool will need to be part of a Skype for Business deployment that includes a Registrar/FE pool that is the next-hop for the VIS pool.

VIS does not support transcoding between RTV and H.264. There is no video interoperability between pre-Lync 2013 clients and VTC participants in a conference.

Having pre-Lync 2013 clients in a conference will cause mobile clients to send using RTV resulting in VTCs receiving no video when the mobile client becomes the dominant speaker.

In order for Lync 2013 to work correctly with VIS that is part of a Skype for Business deployment, Lync 2013 needs the appropriate CU to be applied that upgrades the Lync 2013 client, CAA, and AVMCU to work with VIS.

Interoperability of VIS with Lync 2013 and Skype for Business desktop clients has been tested and is supported.

Interoperability of VIS with non-desktop (Android, Ipad, Iphone, Windows Phone, LMX, etc.) Skype for Business clients available from the applicable Apps Store at the time of VIS release has been tested and is supported.

## Recovery from Packet Loss via FEC

FEC can be turned on to aid in recovery from packet loss. If turned on, 50% more video bandwidth will be used in the VIS to VTC direction.

## VIS Sizing and Transcoding Costs

Transcoding the single video streams from the Cisco VTC to multiple simulcast streams uses CPU capacity. Approximately 16 VTCs can have their video transcoded (assuming a 720p video stream from each VTC is transcoded into 3 separate simulcast streams at 720p, 360p, and 180p) in a single VIS running on the equivalent of the Lync 2013 recommended FE platform. If Transcoding is turned off, this will save on VIS CPU. However, the video image requested by VIS from the VTC will be the lowest common resolution to satisfy all receivers on the Skype for Business side. Note that even with transcoding off, transcoding may be activated when Skype for Business clients request certain low resolutions that VTCs cannot send.

## Call Distribution from the Video Gateway to VIS

Distribution is accomplished via one of the CUCM distribution mechanisms:

- Dynamically using DNS.
- On the CUCM side, you can define individual trunks, where each trunk terminates on a different server in the VIS pool. CUCM will route calls across the different trunks.

## No Hybrid Interoperability

Support for VTCs joining online meetings via on-premises VIS is not part of Skype for Business.



## No Federation Support

Support for VTCs joining federated meetings via VIS is not part of Skype for Business.

## See also

[Deploy Video Interop Server in Skype for Business Server](#)

# Plan your Enterprise Voice solution in Skype for Business Server

7/17/2019 • 2 minutes to read

**Summary:** Learn about your options for planning a unified voice and communications solution in Skype for Business Server.

Skype for Business Server offers two on-premises Enterprise Voice options—Enterprise Voice and Call Via Work—for you to integrate the telephone system of your organization with your Skype for Business Server deployment, making for a true unified communications solution. Both options enable users to use their Skype for Business client to initiate voice calls with other users, both inside and outside of your organization.

You can also take advantage of Microsoft Cloud PBX services, including PBX services and PSTN calling, by connecting your on-premises telephony infrastructure to services provided by Skype for Business Online. For more information, see [Microsoft telephony solutions](#).

You can also use both Enterprise Voice and Call Via Work together.

- Enterprise Voice is the most complete voice offering. It is a software-powered Voice over IP (VoIP) solution, providing a very rich feature set, including rich integration with Outlook and Exchange, and many powerful features such as Response Groups, Call Park, team calling, Group Call Pickup, and Enhanced Emergency E9-1-1 support. With Enterprise Voice, users use an audio device such as a headset with their computer, or a VoIP-enabled phone, instead of a traditional PSTN or PBX phone.
- Call Via Work offers a way for you to integrate your Skype for Business solution with your existing PBX phone systems. A user enabled for Call Via Work can click in Skype for Business to call another user, either within your deployment or an external user. The call is completed using the user's PBX phone. Additionally, these users can click in Skype for Business to join conferences.

Deploying Call Via Work is also a benefit to users who still have PBX phones but are being transitioned to Enterprise Voice, as it enables these users to be using their Skype for Business client to control their phone calls.

Call Via Work offers a more limited set of voice features than Enterprise Voice. For example, it does not support delegation, team call, response group, or Enhanced E9-1-1.

Of course, you can have some of your users enabled for Enterprise Voice while other users are using PBX phones. Additionally, while you transition to a full Enterprise Voice solution, you can enable users who still have PBX phones for Enterprise Voice. These users can use their PBX phone while at their desk, and also use Enterprise Voice to place or receive calls using VoIP devices while in other locations. If these users are enabled for Call Via Work, they can use their Skype for Business client to control their PBX phone while at their desk.

## NOTE

Remote call control was a feature offered in previous versions of Lync Server, enabling users to use their Skype for Business client to make and receive phone calls on their PBX phones. Remote call control is not supported for users homed on Skype for Business Server servers, but is supported for users with Skype for Business clients who are still homed on servers running Lync Server 2013.

See also

[Plan for Enterprise Voice in Skype for Business Server](#)

[Plan for Call Via Work in Skype for Business Server](#)

[Plan for remote call control in Skype for Business](#)

# Plan for Enterprise Voice in Skype for Business Server

5/20/2019 • 3 minutes to read

Enterprise Voice planning basics in Skype for Business Server, including sites, regions, network links between sites, and estimating voice usage traffic.

The deployment process for Enterprise Voice depends on your existing topology, infrastructure, and the Enterprise Voice functionality that you want to support. The required procedures will depend on what features you choose, but there are other planning considerations that you must make at a high level.

In general, consider the type and number of sites that you want to deploy and their geographical locations, the call volume at each site, the types of network links that connect sites, whether you want to provide redundancy and failover for voice functionality for each site, and whether you want to use existing PBX equipment. There are certain considerations, such as high availability, that you should consider when you plan for Skype for Business Server as a whole. These considerations are discussed in topics throughout this section, as needed.

## Sites and regions

First, identify the sites in your topology where you will deploy Enterprise Voice and the network regions to which those sites belong. In particular, consider how you will provide public switched telephone network (PSTN) connectivity to each site. For manageability and logistical reasons, the regions to which these sites belong can be a deciding factor. Decide where gateways will be deployed locally, where Survivable Branch Appliances (SBAs) will be deployed, and where you can configure SIP trunks (either locally or at the central site) to an Internet telephony service provider (ITSP).

## Network links between sites

You also need to consider the bandwidth usage that you expect on the network links between your central site and its branch sites. If you have, or plan to deploy, resilient WAN links between sites, we recommend that you deploy a gateway at each branch site to provide local direct inward dial (DID) termination for users at those sites. If you have resilient WAN links, but the bandwidth on a WAN link is likely to be constrained, configure call admission control for that link. If you do not have resilient WAN links, host fewer than 1000 users at your branch site, and do not have local trained Skype for Business Server administrators available, we recommend that you deploy a Survivable Branch Appliance at the branch site. If you host between 1000 and 5000 users at your branch site, lack a resilient WAN connection, and have trained Skype for Business Server administrators available, we recommend that you deploy a Survivable Branch Server with a small gateway at the branch site. Consider also enabling media bypass on constrained links if you have a gateway peer that supports media bypass.

## Estimating voice usage and traffic

The Microsoft Lync Server 2013, Planning Tool uses the following metric to estimate user traffic at each site and the number of ports that are required to support that traffic.

For **Light traffic** (one PSTN call per user per hour), figure 15 users per port.

For **Medium traffic** (2 PSTN calls per user per hour), figure 10 users per port.

For **Heavy traffic** (3 or more PSTN per user calls per hour), figure 5 users per port.

The number of ports in turn determines the number of Mediation Servers and gateways that will be required. The public switched telephone network (PSTN) gateways that most organizations consider deploying range in size

from 2 ports to as many as 960 ports. (There are even larger gateways, but these are used mainly by telephony service providers.)

For example, an organization with 10,000 users and medium traffic would require 1000 ports. The number of gateways required would equal the total number of ports required as determined by the total capacity of the gateways.

## Components, features, and options of Enterprise Voice

See the following sections for more information on planning your Enterprise Voice deployment.

- [Components required for Enterprise Voice in Skype for Business Server](#)
- [Plan for PSTN connectivity in Skype for Business Server](#)
- [Network settings for the advanced Enterprise Voice features in Skype for Business Server](#)
- [Plan for call admission control in Skype for Business Server](#)
- [Plan for emergency services in Skype for Business Server](#)
- [Plan for media bypass in Skype for Business](#)
- [Plan for private telephone lines with Skype for Business](#)
- [Plan for Location-Based Routing in Skype for Business](#)
- [Plan for call management features in Skype for Business](#)
- [Plan for Enterprise Voice resiliency in Skype for Business Server](#)

# Components required for Enterprise Voice in Skype for Business Server

5/20/2019 • 2 minutes to read

A summary of the Enterprise Voice components in Skype for Business Server.

To deploy Enterprise Voice, the following components are required in your topology.

- One or more Mediation Servers, which translate signaling and, in some configurations, media between your internal Skype for Business Server, Enterprise Voice infrastructure and a public switched telephone network (PSTN) gateway or a Session Initiation Protocol (SIP) trunk. The Mediation Servers are the most crucial component in your Enterprise Voice deployment. For more information, see [Mediation Server component in Skype for Business Server](#).

Mediation Servers can be collocated with Front End Servers or installed as standalone servers.

- PSTN connectivity components, which can include SIP trunks or PSTN gateways. For more information, see [PSTN connectivity components in Skype for Business Server](#).
- Edge Servers, which enables the use of Enterprise Voice features by your users when they are outside your organization's firewall.

The Access Edge service provides SIP signaling for calls from Skype for Business users who are outside your organization's firewall. The A/V Edge service enables media traversal of NAT and firewalls. A caller who uses a unified communications (UC) client from outside the corporate firewall relies on the A/V Edge service for both individual and conference calls.

The A/V Authentication service is collocated with, and provides authentication services for, the A/V Edge service. Outside users who attempt to connect to the A/V Edge service require an authentication token that is provided by the A/V Authentication Service before their calls can go through.

- Additionally, some Enterprise Voice components run on Front End Servers. For details about these components, see [Front End Server VoIP components for Skype for Business Server](#)

# Mediation Server component in Skype for Business Server

5/20/2019 • 15 minutes to read

Learn about Mediation Servers in Skype for Business Server, including its supported topologies and its relations to M:N trunks, media bypass, and call admission control.

To deploy Enterprise Voice, you must deploy one or more Mediation Servers.

The Mediation Server translates signaling between your internal Enterprise Voice infrastructure and a public switched telephone network (PSTN) gateway or a Session Initiation Protocol (SIP) trunk. In some deployments, it also translates the media itself between these points.

On the Skype for Business Server side, Mediation Server listens on a single mutual TLS (MTLS) transport address. On the gateway side, Mediation Server listens on all associated listening ports associated with trunks. All qualified gateways must support TLS, but can enable TCP as well. TCP is supported for gateways that do not support TLS.

If you also have an existing Public Branch Exchange (PBX) in your environment, Mediation Server handles calls between Enterprise Voice users and the PBX. If your PBX is an IP-PBX, you can create a direct SIP connection between the PBX and Mediation Server. If your PBX is a Time Division Multiplex (TDM) PBX, you must also deploy a PSTN gateway between Mediation Server and the PBX.

The Mediation Server is collocated with the Front End Server by default. The Mediation Server can also be deployed in a stand-alone pool.

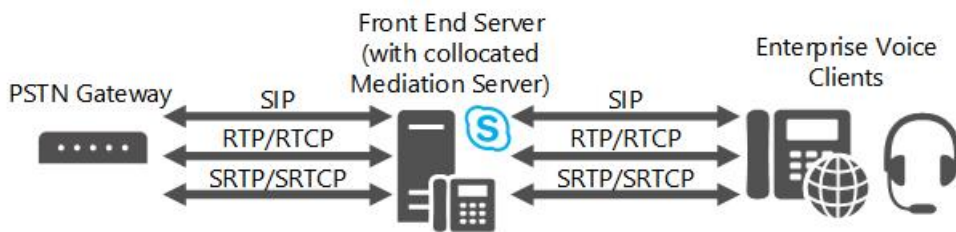
## What Mediation Server Does

The main functions of the Mediation Server are as follows:

- Encrypting and decrypting SRTP on the Skype for Business Server side.
- Translating SIP over TCP (for gateways that do not support TLS) to SIP over mutual TLS.
- Translating media streams between Skype for Business Server and the gateway peer of the Mediation Server.
- Connecting clients that are outside the network to internal ICE components, which enable media traversal of NAT and firewalls.
- Acting as an intermediary for call flows that a gateway does not support, such as calls from remote workers on an Enterprise Voice client.
- In deployments that include SIP trunking, working with the SIP trunking service provider to provide PSTN support, which eliminates the need for a PSTN gateway.

The following figure shows the signaling and media protocols that are used by the Mediation Server when communicating with a basic PSTN gateway and the Enterprise Voice infrastructure.

### **Signaling and media protocols used by the Mediation Server**



#### NOTE

If you are using TCP or RTP/RTCP (instead of SRTP or SRTCP) on the network between the PSTN gateway and the Mediation Server, we recommend that you take measures to help ensure the security and privacy of the network.

## M:N trunk

Skype for Business Server supports flexibility in the definition of a trunk for call routing purposes. A trunk is a logical association between a Mediation Server and listening port number, with a gateway and a listening port number. This implies several things: A Mediation Server can have multiple trunks to the same gateway; a Mediation Server can have multiple trunks to different gateways; conversely a gateway can have multiple trunks to different Mediation Servers.

You must still create a root trunk when you add a gateway to your Skype for Business topology using Topology Builder. The number of gateways that a given Mediation Server can handle depends on the processing capacity of the server during peak busy hours. If you deploy a Mediation Server on hardware that meets the minimum hardware requirements for Skype for Business Server, as described in [Server requirements for Skype for Business Server 2015](#), then a stand-alone Mediation Server can handle approximately 1000 calls. The Mediation Server performs transcoding, but still routes calls for multiple gateways even if the gateways do not support media bypass.

When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with that route. Instead, you use Topology Builder to associate trunks with Mediation Servers. In other words, routing determines which trunk to use for a call, and, subsequently, the Mediation Server associated with that trunk is sent the signaling for that call.

The Mediation Server can be deployed as a pool; this pool can be collocated with a Front End pool, or it can be deployed as a stand-alone pool. When a Mediation Server is collocated with a Front End pool, the pool size can be at most 12 (the limit of the Registrar pool size). Taken together, these capabilities increase the reliability and deployment flexibility for Mediation Servers, but they require similar capabilities in the following:

- PSTN gateway.** A Skype for Business Server qualified gateway must implement DNS load balancing, which enables a qualified public switched telephone network (PSTN) gateway to act as a load balancer for one pool of Mediation Servers, and thereby to load-balance calls across the pool.
- Session Border Controller.** For a SIP trunk, the peer entity is a Session Border Controller (SBC) at an Internet telephony service provider. In the direction from the Mediation Server pool to the SBC, the SBC can receive connections from any Mediation Server in the pool. In the direction from the SBC to the pool, traffic can be sent to any Mediation Server in the pool. One method of achieving this is through DNS load balancing, if supported by the service provider and SBC. An alternative is to give the service provider the IP addresses of all Mediation Servers in the pool, and the service provider will provision these in their SBC as a separate SIP trunk for each Mediation Server. The service provider will then handle the load balancing for its own servers. Not all service providers or SBCs may support these capabilities. Furthermore, the service provider may charge extra for this capability. Typically, each SIP trunk to the SBC incurs a monthly fee.
- IP-PBX.** In the direction from the Mediation Server pool to the IP-PBX SIP termination, the IP-PBX can



receive connections from any Mediation Server in the pool. In the direction from the IP-PBX to the pool, traffic can be sent to any Mediation Server in the pool. Because most IP-PBXs do not support DNS load balancing, we recommend that individual direct SIP connections be defined from the IP-PBX to each Mediation Server in the pool. The IP-PBX will then handle its own load balancing by distributing traffic over the trunk group. The assumption is that the trunk group has a consistent set of routing rules at the IP-PBX. Whether a particular IP-PBX supports this trunk group concept and how it intersects with the IP-PBX's own redundancy and clustering architecture needs to be determined before you can decide whether a Mediation Server cluster can interact correctly with an IP-PBX.

A Mediation Server pool must have a uniform view of the peer gateway with which it interacts. This means that all members of the pool access the same definition of the peer gateway from the configuration store and are equally likely to interact with it for outgoing calls. Therefore, there is no way to segment the pool so that some Mediation Servers communicate with only certain gateway peers for outgoing calls. If such segmentation is necessary, a separate pool of Mediation Servers must be used. This would be the case, for example, if the associated capabilities in PSTN gateways, SIP trunks, or IP-PBXs to interact with a pool as detailed earlier in this topic are not present.

A particular PSTN gateway, IP-PBX, or SIP trunk peer can route to multiple Mediation Servers or trunks. The number of gateways that a particular pool of Mediation Servers can control depends on the number of calls that use media bypass. If a large number of calls use media bypass, a Mediation Server in the pool can handle many more calls, because only signaling layer processing is necessary.

## Call Admission Control and Mediation Server

Call admission control (CAC), manages real-time session establishment, based on available bandwidth, to help prevent poor Quality of Experience (QoE) for users on congested networks. To support this, the Mediation Server is responsible for bandwidth management for its two interactions on the Skype for Business Server side and on the gateway side. In call admission control, the terminating entity for a call handles the bandwidth reservation. The gateway peers (PSTN gateway, IP-PBX, SBC) that the Mediation Server interacts with on the gateway side do not support Skype for Business Server call admission control. Thus, the Mediation Server has to handle bandwidth interactions on behalf of its gateway peer. Whenever possible, the Mediation Server will reserve bandwidth in advance. If that is not possible (for example, if the locality of the ultimate media endpoint on the gateway side is unknown for an outgoing call to the gateway peer), bandwidth is reserved when the call is placed. This behavior can result in oversubscription of bandwidth, but it is the only way to prevent false rings.

Media bypass and bandwidth reservation are mutually exclusive. If media bypass is employed for a call, call admission control is not performed for that call. The assumption here is that there are no links with constrained bandwidth involved in the call. If call admission control is used for a particular call that involves the Mediation Server, that call cannot employ media bypass.

For details about media bypass or call admission control, see [Plan for media bypass in Skype for Business](#) or [Plan for call admission control in Skype for Business Server](#).

## Enhanced 9-1-1 (E9-1-1) and Mediation Server

The Mediation Server has extended capabilities so that it can correctly interact with Enhanced 9-1-1 (E9-1-1) service providers. No special configuration is needed on the Mediation Server. The SIP extensions required for E9-1-1 interaction are, by default, included in the Mediation Server's SIP protocol for its interactions with a gateway peer (PSTN gateway, IP-PBX, or the SBC of an Internet Telephony Service Provider, including E9-1-1 Service Providers)

Whether the SIP trunk to an E9-1-1 Service Provider can be terminated on an existing Mediation Server pool or will require stand-alone Mediation Servers will depend on whether the E9-1-1 SBC can interact with a pool of Mediation Servers. For details, see [M:N trunk in Skype for Business Server](#).

# Media bypass and Mediation Server

Media bypass is a Skype for Business Server capability that enables an administrator to configure call routing to flow directly between the user endpoint and the public switched telephone network (PSTN) gateway without traversing the Mediation Server. Media bypass improves call quality by reducing latency, unnecessary translation, possibility of packet loss, and the number of potential points of failure. Where a remote site without a Mediation Server is connected to a central site by one or more WAN links with constrained bandwidth, media bypass lowers the bandwidth requirement by enabling media from a client at a remote site to flow directly to its local gateway without first having to flow across the WAN link to a Mediation Server at the central site and back. This reduction in media processing also complements the Mediation Server's ability to control multiple gateways.

Media bypass and call admission control (CAC) are mutually exclusive. If media bypass is employed for a call, CAC is not performed for that call. The assumption is that there are no links with constrained bandwidth involved in the call.

## Topologies for Mediation Server

The Skype for Business Server, Mediation Server is by default collocated with Standard Edition server, a Front End pool, or Survivable Branch Appliance. All Mediation Servers in a Front End pool must be configured identically.

Where performance is an issue, it may be preferable to deploy one or more Mediation Servers in a dedicated stand-alone pool. We definitely recommend a stand-alone pool if you are deploying SIP trunking.

If you deploy Direct SIP connections to a qualified PSTN gateway that supports media bypass and DNS load balancing, a stand-alone Mediation Server pool is not necessary. This is because qualified gateways are capable of DNS load balancing to a pool of Mediation Servers and they can receive traffic from any Mediation Server in a pool.

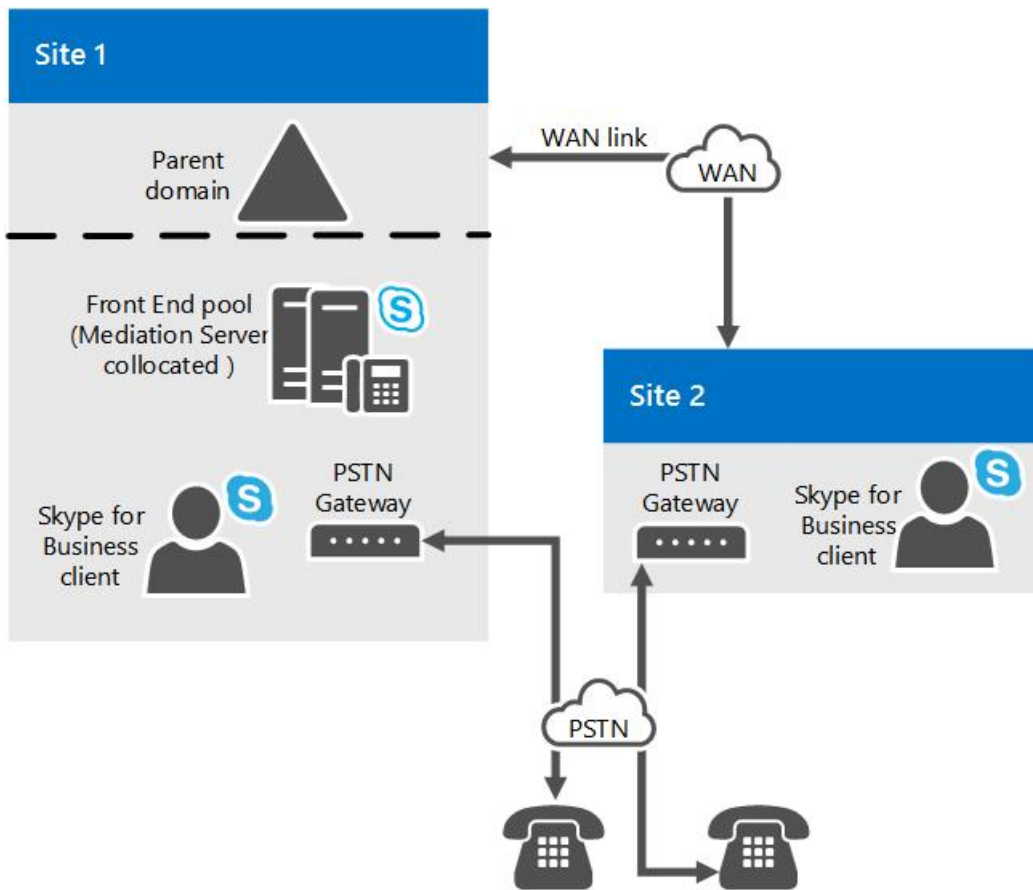
We also recommend that you collocate the Mediation Server on a Front End pool when you have deployed IP-PBXs or connect to an Internet Telephony Server Provider's Session Border Controller (SBC), as long as any of the following conditions are met:

- The IP-PBX or SBC is configured to receive traffic from any Mediation Server in the pool and can route traffic uniformly to all Mediation Servers in the pool.
- The IP-PBX does not support media bypass, but the Front End pool that is hosting the Mediation Server can handle voice transcoding for calls to which media bypass does not apply.

You can use the Microsoft Lync Server 2013, Planning Tool to evaluate whether the Front End pool where you want to collocate the Mediation Server can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

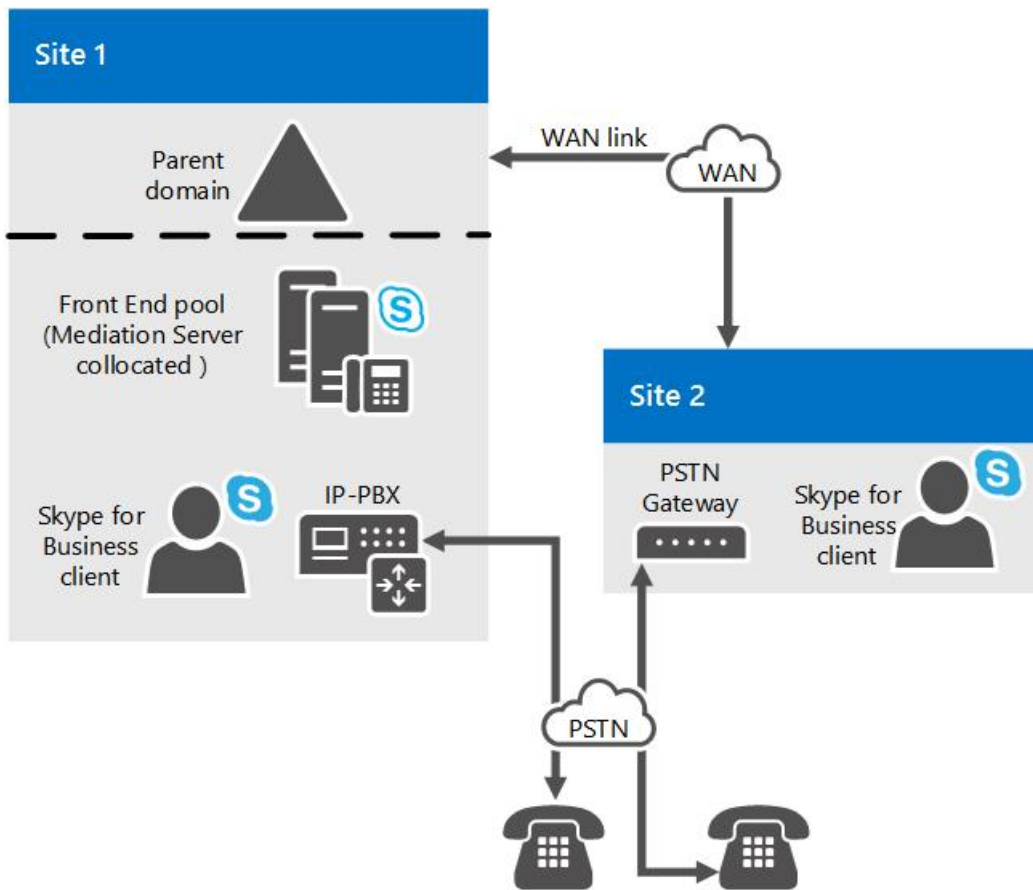
The following figure shows a simple topology consisting of two sites connected by a WAN link. Mediation Server is collocated on a Front End pool at Site 1. The Mediation Servers at Site 1 controls both the PSTN gateway at Site 1 and the gateway at Site 2. In this topology, media bypass is enabled globally to use site and region information, and the trunks to each PSTN gateway (GW1 and GW2) have bypass enabled.

**Example of sites connected by a WAN link with a Mediation Server at Site 1 and a PSTN gateway at Site 2**



The next figure shows a simple topology where Mediation Server is collocated on Front End pool at Site 1 and has a Direct SIP connection to the IP-PBX at Site 1. In this figure, the Mediation Server also controls a PSTN gateway at Site 2. Assume that Skype for Business users exist at both Sites 1 and 2. Also assume that the IP-PBX has an associated media processor that must be traversed by all media originating from Skype for Business endpoints before being sent to media endpoints controlled by the IP-PBX. In this topology, media bypass is enabled globally to use site and region information, and the trunks to the PBX and PSTN gateway have media bypass enabled.

**Example of sites connected by a WAN link with a Mediation Server at Site 1 and a PBX at Site 2**



The last figure in this topic shows a topology where the Mediation Server is connected to the SBC of an Internet Telephony Service Provider.

## Planning decisions for Mediation Server

This topic describes planning decisions you need to make for your Mediation Server deployment,

### Collocated or Stand-alone Mediation Server?

Mediation Server is by default collocated on the Standard Edition server or Front End Server in a Front End pool at central sites. The number of public switched telephone network (PSTN) calls that can be handled and the number of machines required in the pool will depend on the following:

- The number of gateway peers that the Mediation Server pool controls
- The high-volume traffic periods through those gateways
- The percentage of calls that are calls whose media bypass the Mediation Server

When planning, be sure to take into account the media processing requirements for PSTN calls and A/V conferences that are not configured for media bypass, as well as the processing needed to handle signaling interactions for the number of busy-hour calls that need to be supported. If there is not enough CPU, then you must deploy a stand-alone pool of Mediation Servers; and PSTN gateways, IP-PBXs, and SBCs will need to be split into subsets that are controlled by the collocated Mediation Servers in one pool and the stand-alone Mediation Servers in one or more stand-alone pools.

If you deployed PSTN gateways, IP-PBXs, or Session Border Controllers (SBCs) that do not support the correct capabilities to interact with a pool of Mediation Servers, including the following, then they will need to be associated with a stand-alone pool consisting of a single Mediation Server:

- Perform network layer Domain Name System (DNS) load balancing across Mediation Servers in a pool (or otherwise route traffic uniformly to all Mediation Servers in a pool)

- Accept traffic from any Mediation Server in a pool

You can use the Microsoft Lync Server 2013, Planning Tool to evaluate whether collocating the Mediation Server with your Front End pool can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

### Central Site and Branch Site Considerations

Mediation Servers at the central site can be used to route calls for IP-PBXs or PSTN gateways at branch sites. If you deploy SIP trunks, however, you must deploy a Mediation Server at the site where each trunk terminates. Having a Mediation Server at the central site route calls for an IP-PBX or PSTN gateway at a branch site does not require the use of media bypass. However, if you can enable media bypass, doing so will reduce media path latency and improve the media quality because the media path is no longer required to follow the signaling path. Media bypass also decreases the processing load on the pool.

#### NOTE

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed at [Unified Communications Open Interoperability Program - Lync Server](#).

If branch site resiliency is required, a Survivable Branch Appliance or combination of a Front End Server, a Mediation Server, and a gateway must be deployed at the branch site. (The assumption with branch site resiliency is that presence and conferencing are not resilient at the site.) For guidance on branch site planning for voice, see [Plan for Enterprise Voice resiliency in Skype for Business Server](#).

For interactions with an IP-PBX, if the IP-PBX does not correctly support early media interactions with multiple early dialogs and RFC 3960 interactions, there can be clipping of the first few words of the greeting for incoming calls from the IP-PBX to Skype for Business endpoints. This issue can be more severe if a Mediation Server at a central site is routing calls for an IP-PBX where the route terminates at a branch site, because more time is needed for signaling to complete. If you experience this behavior, deploying a Mediation Server at the branch site is the only way to reduce clipping of the first few words.

Finally, if your central site has a TDM PBX, or if your IP-PBX does not eliminate the need for a PSTN gateway, then you must deploy a gateway on the call route connecting Mediation Server and the PBX.

#### NOTE

To improve the media performance of standalone Mediation Server, you should enable receive-side scaling (RSS) on the network adapters on these servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "[Receive-Side Scaling Enhancements in Windows Server](#)". For details about how to enable RSS, see your network adapter documentation.

# PSTN connectivity components in Skype for Business Server

5/20/2019 • 2 minutes to read

Learn about SIP trunking and PSTN gateways for Enterprise Voice in Skype for Business Server.

An enterprise-grade VoIP solution must provide for calls to and from the public switched telephone network (PSTN) without any decline in Quality of Service (QoS). In addition, users should not be aware of the underlying technology when they place and receive calls. From the user's perspective, a call between the Enterprise Voice infrastructure and the PSTN should seem like just another SIP session.

For PSTN connections, you can either deploy a SIP trunk or a PSTN gateway (with a PBX, also known as a Direct SIP link, or without a PBX).

## SIP Trunking

As an alternative to using PSTN gateways, you can connect your Enterprise Voice solution to the PSTN by using SIP trunking. SIP trunking enables the following scenarios:

- An enterprise user inside or outside the corporate firewall can make a local or long-distance call specified by an E.164-compliant number that is terminated on the PSTN as a service of the corresponding service provider.
- Any PSTN subscriber can contact an enterprise user inside or outside the corporate firewall by dialing a Direct Inward Dialing (DID) number associated with that enterprise user.

The use of this deployment solution requires a SIP trunking service provider.

## PSTN gateways

PSTN gateways are third-party devices that translate signaling and media between the Enterprise Voice infrastructure and a PSTN or a PBX. PSTN gateways work with the Mediation Server to present a PSTN or PBX call to an Enterprise Voice client. The Mediation Server also presents calls from Enterprise Voice clients to the PSTN gateway for routing to the PSTN or PBX. For a list of partners who work with Microsoft to provide devices that work with Skype for Business Server, see [the Microsoft Unified Communications Partners website](#).

## Private Branch Exchanges

If you have an existing voice infrastructure that uses a private branch exchange (PBX), you can use your PBX with Enterprise Voice.

The supported Enterprise Voice-PBX integration scenarios are as follows:

- IP-PBX that supports media bypass, with a Mediation Server.
- IP-PBX that requires a stand-alone PSTN gateway.
- Time division multiplexing (TDM) PBX, with a stand-alone PSTN gateway.

**NOTE**

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed at [Unified Communications Open Interoperability Program - Lync Server](#).

For details about partners who offer Enterprise Voice solutions, see the [Microsoft Unified Communications Partners website](#).

For details about partners who offer Enterprise Voice hardware solutions, including PSTN gateways, see the [Microsoft Unified Communications Partners website](#).

# Front End Server VoIP components for Skype for Business Server

5/20/2019 • 4 minutes to read

Learn about the Enterprise Voice components that are located on Front End Servers in Skype for Business Server, including translation service and various routing components.

The VoIP components located on Front End Servers are as follows:

- Translation Service
- Inbound Routing component
- Outbound Routing component
- Exchange UM Routing component
- Intercluster Routing component
- [Mediation Server component in Skype for Business Server](#)

## Translation Service

The Translation Service is the server component that is responsible for translating a dialed number into the E.164 format or another format, according to the normalization rules that are defined by the administrator. The Translation Service can translate to formats other than E.164 if your organization uses a private numbering system or uses a gateway or PBX that does not support E.164.

## Inbound Routing Component

The Inbound Routing component handles incoming calls largely according to preferences that are specified by users on their Enterprise Voice clients. It also facilitates delegate ringing and simultaneous ringing, if configured by the user. For example, users specify whether unanswered calls are forwarded or simply logged for notification. If call forwarding is enabled, users can specify whether unanswered calls should be forwarded to another number or to a Exchange UM server that has been configured to provide call answering. The Inbound Routing component is installed by default on all Standard Edition server and Front End Servers.

## Outbound Routing Component

The Outbound Routing component routes calls to PBX or PSTN destinations. It applies call authorization rules, as defined by the user's voice policy, to callers and determines the optimal PSTN gateway for routing each call. The Outbound Routing component is installed by default on all Standard Edition server and Front End Servers.

The routing logic that is used by the Outbound Routing component is in large measure configured by network or telephony administrators according to the requirements of their organizations.

## Exchange UM Routing Component

The Exchange UM routing component handles routing between Skype for Business Server and servers running Exchange Unified Messaging (UM), to integrate Skype for Business Server with Unified Messaging features.

The Exchange UM routing component also handles rerouting of voice mail over the PSTN if Exchange UM servers



are unavailable. If you have Enterprise Voice users at branch sites that do not have a resilient WAN link to a central site, the Survivable Branch Appliance that you deploy at the branch site provides voice mail survivability for branch users during a WAN outage. When the WAN link is unavailable, the Survivable Branch Appliance does the following:

- reroutes unanswered calls over the PSTN to the Exchange Unified Messaging server in the central site
- provides the ability for a user to retrieve voice mail messages over the PSTN
- queues missed call notifications, and then uploads them to the Exchange UM server when the WAN link is restored.

To enable voice mail rerouting, we recommend that your Exchange administrator configure Exchange UM Auto Attendant (AA) to accept messages only.

For details about these features, see [On-Premises Exchange Unified Messaging Integration](#) and [Planning for Enterprise Voice Resiliency](#), respectively.

## Intercluster Routing Component

The Intercluster routing component is responsible for routing calls to the callee's primary Registrar pool. If that is unavailable, the component routes the call to the callee's backup Registrar pool. If the callee's primary and backup Registrar pools are unreachable over the IP network, the Intercluster routing component reroutes the call over the PSTN to the user's telephone number.

## Other Front End Server Components Required for VoIP

Other components residing on the Front End Server or Director that provide essential support for VoIP, but are not themselves VoIP components, include the following:

- **User Services.** Perform reverse number lookup on the destination phone number of each incoming call and match that number to the SIP URI of the destination user. Using this information, the Inbound Routing component distributes the call to that user's registered SIP endpoints. User Services is a core component on all Front End Servers and Directors.
- **User Replicator.** Extracts user phone numbers from Active Directory Domain Services and writes them to tables in the RTC database, where they are available to User Services and Address Book Server. User Replicator is a core component on all Front End Servers.
- **Address Book Server.** Provides global address list information from Active Directory Domain Services to Skype for Business Server clients. It also retrieves user and contact information from the RTC database, writes the information to the Address Book files, and then stores the files on a shared folder where they are downloaded by Skype for Business clients. The Address Book Server writes the information to the RTCAb database, which is used by the Address Book Web Query service to respond to user search queries from Skype for Business mobile. It optionally normalizes enterprise user phone numbers that are written to the RTC database for the purpose of provisioning user contacts in Skype for Business. The Address Book service is installed by default on all Front End Servers. The Address Book Web Query service is installed by default with the Web services on each Front End Servers.

# Plan for PSTN connectivity in Skype for Business Server

5/20/2019 • 2 minutes to read

Plan for PSTN connectivity in Enterprise Voice in Skype for Business Server.

An enterprise-grade VoIP solution must provide for calls to and from the public switched telephone network (PSTN) without any decline in Quality of Service (QoS). Users who place and receive calls should not be aware of the underlying technology: from the user's perspective, a call between the Enterprise Voice infrastructure and the PSTN should seem like just another phone call.

Skype for Business Server provides reliable, scalable PSTN connectivity by using the following options:

- **SIP trunks** to an Internet telephony service provider (ITSP)
- **Direct SIP connections** to a PSTN gateway
- **Direct SIP connections** to a PBX

Depending on its size, geographic coverage, and existing voice infrastructure, an enterprise may use one, two, or even all three of these options at various locations. For details about these options, see the following sections.

## In this section

- [SIP trunking in Skype for Business Server](#)
- [Direct SIP connections in Skype for Business Server](#)
- [M:N trunk in Skype for Business Server](#)
- [Translation rules in Skype for Business Server](#)
- [Plan for outbound voice routing in Skype for Business Server](#)

# SIP trunking in Skype for Business Server

5/20/2019 • 10 minutes to read

Learn about SIP trunking in Skype for Business Server Enterprise Voice

Session Initiation Protocol (SIP) is used to initiate and manage Voice over IP (VoIP) communications sessions for basic telephone service and for additional real-time communication services, such as instant messaging, conferencing, presence detection, and multimedia. This section provides planning information for implementing SIP trunks, a type of SIP connection that extends beyond the boundary of your local network.

## What is SIP Trunking?

A SIP trunk is an IP connection that establishes a SIP communications link between your organization and an Internet telephony service provider (ITSP) beyond your firewall. Typically, a SIP trunk is used to connect your organization's central site to an ITSP. In some cases, you may also opt to use SIP trunking to connect your branch site to an ITSP.

Deploying SIP trunking can be a big step toward simplifying your organization's telecommunications and preparing for up-to-date enhancements to real-time communications. One of the primary advantages of SIP trunking is that you can consolidate your organization's connections to the public switched telephone network (PSTN) at a central site, as opposed to its predecessor, time division multiplexing (TDM) trunking, which typically requires a separate trunk from each branch site.

### Cost Savings

The cost savings associated with SIP trunking can be substantial:

- Long distance calls typically cost much less through a SIP trunk.
- You can cut manageability costs and reduce the complexity of deployment.
- Basic rate interface (BRI) and primary rate interface (PRI) fees can be eliminated if you connect a SIP trunk directly to your ITSP at significantly lower cost. In TDM trunking, service providers charge for calls by the minute. The cost of SIP trunking may be based on bandwidth usage, which you can buy in smaller, more economical increments. (The actual cost depends on the service model of the ITSP you choose.)

### SIP Trunking vs. Hosting a PSTN Gateway or IP-PBX

Because SIP trunks connect directly to your service provider, you can eliminate your PSTN gateways and their management cost and complexity. Using a SIP trunk can lead to substantial cost savings through reduced maintenance and administration.

### Expanded VoIP Services

Voice features are often the primary motivation for deploying SIP trunking, but voice support is just the first step. With SIP trunking, you can extend VoIP capabilities and enable Skype for Business Server to deliver a richer set of services. For example:

- Enhanced presence detection for devices that are not running Skype for Business Server can provide better integration with mobile phones, enabling you to see when a user is on a mobile phone call.
- E9-1-1 emergency calling enables the authorities who answer 911 calls to determine the caller's location from his or her telephone number.

## NOTE

Contact your ITSP for a list of services that they support and can enable for your organization.

### SIP Trunks vs. Direct SIP Connections

The term trunk is derived from circuit-switched technology. It refers to a dedicated physical line that connects telephone switching equipment. Like their predecessor, time division multiplexing (TDM) trunks, SIP trunks are connections between two separate SIP networks—the Skype for Business Server enterprise and the ITSP. Unlike circuit-switched trunks, SIP trunks are virtual connections that can be established over any of the supported SIP trunking connection types.

Direct SIP connections, on the other hand, are SIP connections that do not cross the local network boundary (that is, they connect to a public switched telephone network (PSTN) gateway or private branch exchange (PBX) within your internal network). For details about how you can use direct SIP connections with Skype for Business Server, see [Direct SIP connections in Skype for Business Server](#).

## How do I implement SIP Trunking?

To implement SIP trunking, you must route the connection through a Mediation Server, which acts as a proxy for communications sessions between Skype for Business Server clients and the service provider and transcodes media, when necessary.

Each Mediation Server has an internal network interface and an external network interface. The internal interface connects to the Front End Servers. The external interface is commonly called the gateway interface because it has traditionally been used to connect the Mediation Server to a public switched telephone network (PSTN) gateway or an IP-PBX. To implement a SIP trunk, you connect the external interface of the Mediation Server to the external edge component of the ITSP. The external edge component of the ITSP could be a Session Border Controller (SBC), a router, or a gateway.

For details about Mediation Servers, see [Mediation Server component in Skype for Business Server](#).

### Centralized vs. Distributed SIP Trunking

Centralized SIP trunking routes all VoIP traffic, including branch site traffic, through your central site. The centralized deployment model is simple, cost-effective, and is generally the recommended approach for implementing SIP trunks with Skype for Business Server.

Distributed SIP trunking is a deployment model in which you implement local SIP trunks at one or more branch sites. VoIP traffic is then routed from the branch site directly to a service provider without going through the central site.

Distributed SIP trunking is required only in the following cases:

- The branch site requires survivable phone connectivity (for example, if the WAN goes down). This requirement should be analyzed for each branch site; some of your branches may require redundancy and failover, whereas others may not.
- Resiliency is required between two central sites. You need to make sure that a SIP trunk terminates at each central site. For example, if you have Dublin and Tukwila central sites and both use only one site's SIP trunk, if the trunk goes down, the other site's users cannot make PSTN calls.
- The branch site and central site are in different countries/regions. For compatibility and legal reasons, you need at least one SIP trunk per country/region. For example, in the European Union, communications cannot leave a country/region without terminating locally at a centralized point.

Depending on the geographical location of sites and how much traffic you anticipate within your enterprise, you may not want to route all users through the central SIP trunk, or you may opt to route some users through a SIP

trunk at their branch site. To analyze your needs, answer the following questions:

- How big is each site (that is, how many users are enabled for Enterprise Voice)?
- Which direct inward dialing (DID) numbers at each site get the most phone calls?

The decision whether to deploy centralized or distributed SIP trunking requires a cost-benefit analysis. In some cases, it may be advantageous to opt for the distributed deployment model even if it is not required. In a completely centralized deployment, all branch site traffic is routed over WAN links. Instead of paying for the bandwidth required for WAN linking, you may want to use distributed SIP trunking. For example, you may want to deploy a Standard Edition server at a branch site with federation to the central site, or you may want to deploy a Survivable Branch Appliance or a Survivable Branch Server with a small gateway.

#### NOTE

For details about distributed SIP trunking, see [Branch site SIP trunking in Skype for Business Server](#).

### Supported SIP Trunking Connection Types

Skype for Business Server supports the following connection types for SIP trunking:

- Multiprotocol Label Switching (MPLS) is a private network that directs and carries data from one network node to the next. The bandwidth in an MPLS network is shared with other subscribers, and each data packet is assigned a label to distinguish one subscriber's data from another's. This connection type does not require a virtual private network (VPN). A potential drawback is that excessive IP traffic can interfere with VoIP operation unless VoIP traffic is given priority.
- A private connection with no other traffic—for example, a leased fiber-optic connection or T1 line—is typically the most reliable and secure connection type. This connection type provides the highest call-carrying capacity, but it is typically the most expensive. VPN is not required. Private connections are appropriate for organizations with high call volumes or stringent security and availability requirements.
- The Internet is the least expensive connection type, but it is also the least reliable. Internet connection is the only Skype for Business Server SIP trunking connection type that requires VPN.

#### Selecting a Connection Type

The most appropriate SIP trunking connection type for your enterprise depends on your needs and your budget.

- For a mid-size or larger enterprise, an MPLS network usually provides the greatest value. It can provide the necessary bandwidth at a cheaper rate than a specialized private network.
- Large enterprises may require a private fiber-optic, T1, T3 or higher connection (E1, E3 or higher in the European Union).
- For a small enterprise or branch site with low call volume, SIP trunking through the Internet may be the best choice. This connection type is not recommended for mid-size or larger sites.

### Bandwidth Requirements

The amount of bandwidth your implementation requires depends on call capacity (the number of concurrent calls you must be able to support). You need to consider bandwidth availability, so that you can take full advantage of the peak capacity that you have paid for. Use the following formula to calculate SIP trunk peak bandwidth requirement:

SIP Trunk Peak Bandwidth = Max Simultaneous Calls x (64 kbps + header size)

**NOTE**

Header size is 20 bytes maximum.

**Codec Support**

Skype for Business Server supports only the following codecs:

- G.711 a-law (used primarily outside North America)
- G.711  $\mu$ -law (used in North America)

**Internet Telephony Service Provider**

How you implement the service provider side of a SIP trunk connection varies from one ITSP to another. For deployment information, contact your service provider. For a list of certified SIP trunking service providers, see [Microsoft Unified Communications Open Interoperability Program website](#).

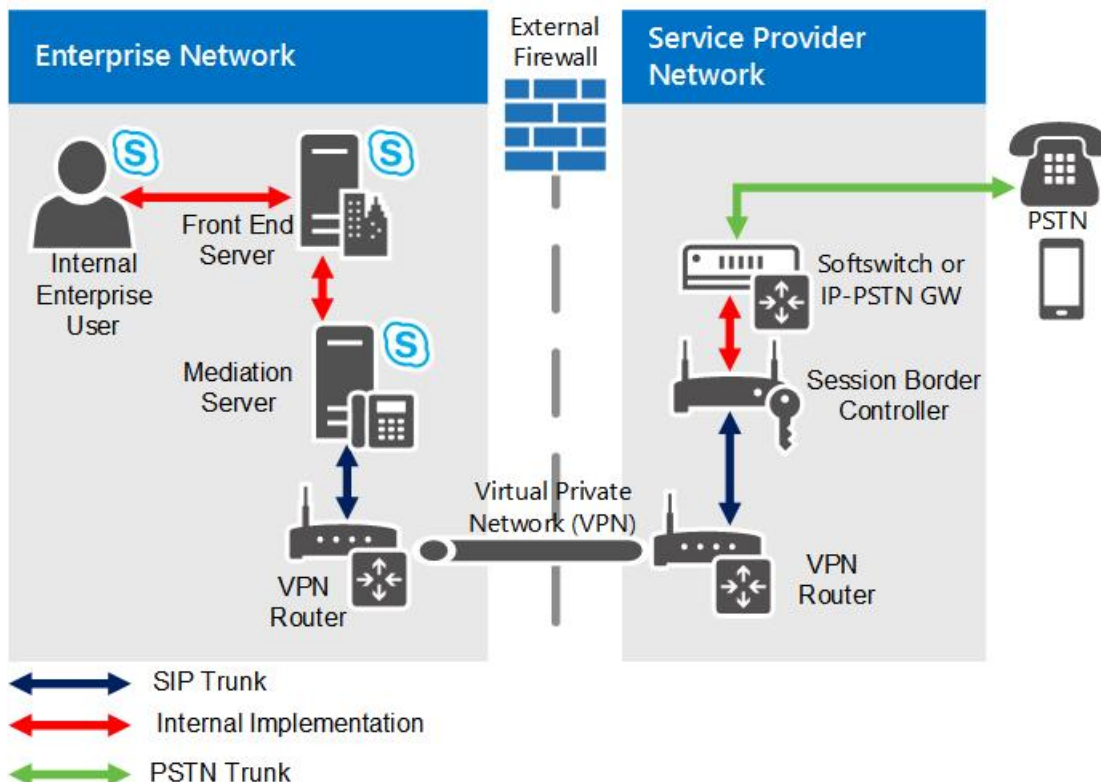
For details about Microsoft certified SIP trunking providers, contact your Microsoft representative.

**IMPORTANT**

You must use a Microsoft certified service provider to ensure that your ITSP supports all of the functionality that traverses the SIP trunk (for example, setting up and managing sessions and supporting all of the extended VoIP services). Microsoft technical support does not extend to configurations that use noncertified providers. If you currently use an Internet service provider that is not certified for SIP trunking, you can opt to continue using that provider as your ISP and use a provider certified by Microsoft for SIP trunking.

**Topologies and Components for SIP Trunking**

The following figure depicts the SIP trunking topology in Skype for Business Server.

**SIP trunking topology**

As shown in the diagram, an IP virtual private network (VPN) is used for connectivity between the enterprise network and the public switched telephone network (PSTN) service provider. The purpose of this private network

is to provide IP connectivity, enhance security, and (optionally) obtain Quality of Service (QoS) guarantees. Because of the nature of a VPN, you do not need to use Transport Layer Security (TLS) for SIP signaling traffic or secure real-time transport protocol (SRTP) for the media traffic. Connections between the enterprise and the service provider therefore consist of plain TCP connections for SIP and plain real-time transport protocol (RTP) (over UDP) for media tunneled through an IP VPN. Ensure that all firewalls between the VPN routers have ports open to allow the VPN routers to communicate, and that the IP addresses on the external edges of the VPN routers are publicly routable.

#### **IMPORTANT**

Contact your service provider to determine whether it provides support for high availability, including failover. If so, you will need to determine the procedures for setting it up. For example, do you need to configure only one IP address and one SIP trunk on each Mediation Server, or do you need to configure multiple SIP trunks on each Mediation Server? > If you have multiple central sites, also ask whether the service provider has the ability to enable connections to and from another central site.

#### **NOTE**

For SIP trunking, we strongly recommend that you deploy stand-alone Mediation Servers. For details, see [Deploying Mediation Servers and Defining Peers](#) in the Deployment documentation.

### **Securing the Mediation Server for SIP Trunking**

For security purposes, you should set up a virtual LAN (VLAN) for each connection between the two VPN routers. The actual process for setting up a VLAN varies from one router manufacturer to another. For details, contact your router vendor.

We recommend that you follow these guidelines:

- Set up a virtual LAN (VLAN) between the Mediation Server and the VPN router in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet).
- Do not allow broadcast or multicast packets to be transferred from the router to the VLAN.
- Block any routing rules that route traffic from the router to anywhere but the Mediation Server.

If you use a VPN server, we recommend that you follow these guidelines:

- Set up a VLAN between the VPN server and the Mediation Server.
- Do not allow broadcast or multicast packets to be transmitted from the VPN server to the VLAN.
- Block any routing rule that routes VPN server traffic to anywhere but the Mediation Server.
- Encrypt data on the VPN by using generic routing encapsulation (GRE).

## **See also**

[Branch site SIP trunking in Skype for Business Server](#)

# Branch site SIP trunking in Skype for Business Server

5/20/2019 • 2 minutes to read

Learn about SIP trunking at branch sites in Skype for Business Server Enterprise Voice.

In some cases, you may need to implement distributed SIP trunking at selected branch sites. To determine whether a SIP trunk is needed for a branch site, and for details about the supported topology options for deploying SIP trunks in branch sites, see [SIP trunking in Skype for Business Server](#).

## Example Branch Site SIP Trunk Requirements Analysis

When you decide to deploy a branch site SIP trunk, you need to perform a site-specific cost analysis. For example, an enterprise that has a central site in Redmond, Washington, and a branch site in New York, should do an analysis to determine whether to implement a SIP trunk from the New York site to a local service provider.

To determine whether a distributed SIP trunk in New York is cost-effective, identify which Direct Inward Dialing (DID) numbers will use the SIP trunk, and analyze the number of calls New York makes to areas other than Redmond (425). You can have DID termination for the branch site at the central site. For example, the Redmond central site can host DID numbers for the New York branch site. If the cost of implementing a distributed SIP trunk is less than the cost of those calls, consider implementing a SIP trunk at the New York branch site.

## Other Branch Site SIP Trunk Requirements

The choice between a deploying a SIP trunk instead of a gateway is based on the difference between the public switched telephone network (PSTN) long distance toll charges of each option. If you deploy a branch site SIP trunk, you also need to determine your resiliency and bandwidth requirements. If the link between your branch site and central site is resilient and has sufficient bandwidth, you can deploy a SIP trunk or a gateway. You do not need to deploy a Survivable Branch Appliance at the branch site. If the link between your branch site and central site is not resilient, deploy a Survivable Branch Appliance, or deploy a Survivable Branch Server with either a gateway or SIP trunk at the branch site.



# Direct SIP connections in Skype for Business Server

5/20/2019 • 10 minutes to read

Direct SIP connections are supported between Skype for Business Server and both PSTN gateways and IP-PBX in Enterprise Voice.

You can use direct SIP connections to connect Skype for Business Server to either of the following:

- An IP-PBX
- A PSTN gateway

To implement a direct SIP connection, you follow essentially the same deployment steps as you would to implement a SIP trunk. In both cases, you implement the connection by using the external interface of a Mediation Server. The only difference is that you connect SIP trunks to an external entity, such as an ITSP gateway, and you connect direct SIP connections to an internal entity within your local network, such as an IP-PBX or a public switched telephone network (PSTN) gateway.

## Direct SIP deployment options

### Skype for Business Server Stand-Alone

If your organization uses one of the deployments described in this section, you can use Skype for Business Server as the sole telephony solution for part or all of an organization. This section describes the following deployments in detail:

- **Incremental deployment:** This option assumes that you have an existing private branch exchange (PBX) infrastructure and you intend to introduce Enterprise Voice incrementally to smaller groups or teams within your organization.
- **VoIP-only deployment:** this option assumes that you are considering deploying Enterprise Voice at a site that does not have a traditional telephony infrastructure.

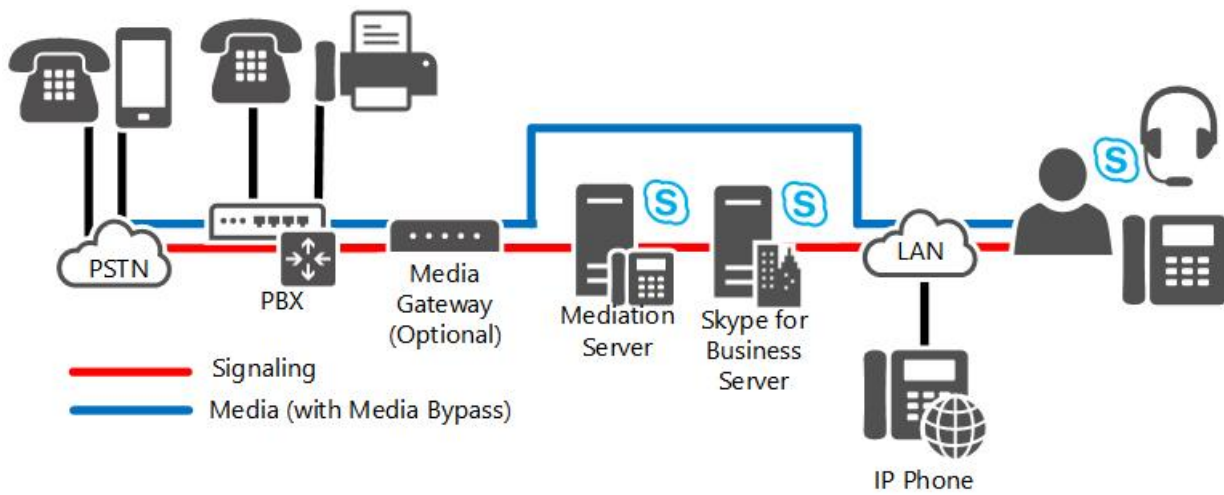
#### Incremental Deployment

In incremental deployment, Skype for Business Server is the sole telephony solution for individual teams or departments, while the rest of the users in an organization continue to use a PBX. This incremental deployment strategy provides one way to introduce IP telephony into your enterprise through controlled pilot programs. Workgroups whose communication needs are best served by Microsoft Unified Communications are moved to Enterprise Voice, while other users remain on the existing PBX. Additional workgroups can be migrated to Enterprise Voice, as needed.

The incremental option is recommended if you have clearly defined user groups that have communication requirements in common and that lend themselves to centralized management. This option is also effective if you have teams or departments that are spread over wide geographic areas, where the savings in long-distance charges can be significant. In fact, this option is useful for creating virtual teams whose members may be scattered across the globe. You can create, modify, or disband such teams in rapid response to shifting business requirements.

The following figure shows the generic topology for deployment of Enterprise Voice behind a PBX. This is the recommended topology for incremental deployment.

#### Incremental deployment option



#### NOTE

If you are connecting your Skype for Business Server deployment to a certified Direct SIP partner, a public switched telephone network (PSTN) gateway between the Mediation Server and the PBX is not required. For a list of certified Direct SIP partners, see the [Microsoft Unified Communications Open Interoperability Program](#).

#### NOTE

The media path shown in this figure has media bypass enabled (the recommended configuration). If you opt to disable media bypass, the media path is routed through the Mediation Server.

In this topology, selected departments or workgroups are enabled for Enterprise Voice. A PSTN gateway links the Voice over Internet Protocol (VoIP)-enabled workgroup to the PBX. Users who are enabled for Enterprise Voice, including remote workers, communicate across the IP network. Calls by Enterprise Voice users to the PSTN and to coworkers who are not enabled for Enterprise Voice are routed to the appropriate PSTN gateway. Calls from colleagues who are still on the PBX system, or from callers on the PSTN, are routed to the PSTN gateway, which forwards the calls to Skype for Business Server for routing.

There are two recommended configurations for connecting Enterprise Voice to an existing PBX infrastructure for interoperability: Enterprise Voice behind the PBX and Enterprise Voice in front of the PBX.

#### Enterprise Voice Behind the PBX

When Enterprise Voice is deployed behind the PBX, all calls from the PSTN arrive at the PBX, which routes calls to Enterprise Voice users to a PSTN gateway, and calls to PBX users to the PBX.

#### Enterprise Voice in Front of the PBX

When Enterprise Voice is deployed in front of the PBX, all calls arrive at the PSTN gateway, which routes calls for Enterprise Voice users to Skype for Business Server and calls for PBX users to the PBX. Calls to the PSTN from both Enterprise Voice and PBX users are routed over the IP network to the most cost-efficient PSTN gateway. The following table shows the advantages and disadvantages of this configuration.

#### Advantages and Disadvantages of Deploying Enterprise Voice in Front of PBX

ADVANTAGES	DISADVANTAGES
PBX still serves users not enabled for Enterprise Voice.	Existing gateways may not support the features or capacity that you want.

ADVANTAGES	DISADVANTAGES
PBX handles all earlier devices.	Requires a trunk from gateway to the PBX and from the gateway to the Mediation Server. You may need more trunks from the service provider.
Enterprise Voice users keep the same phone numbers.	

### VoIP-Only Deployment

Enterprise Voice provides new businesses, and also new office sites for existing businesses, with the opportunity to implement a full-featured VoIP solution without having to worry about PBX integration or incurring the substantial deployment and maintenance costs of an IP-PBX infrastructure. This solution supports both on-site and remote workers.

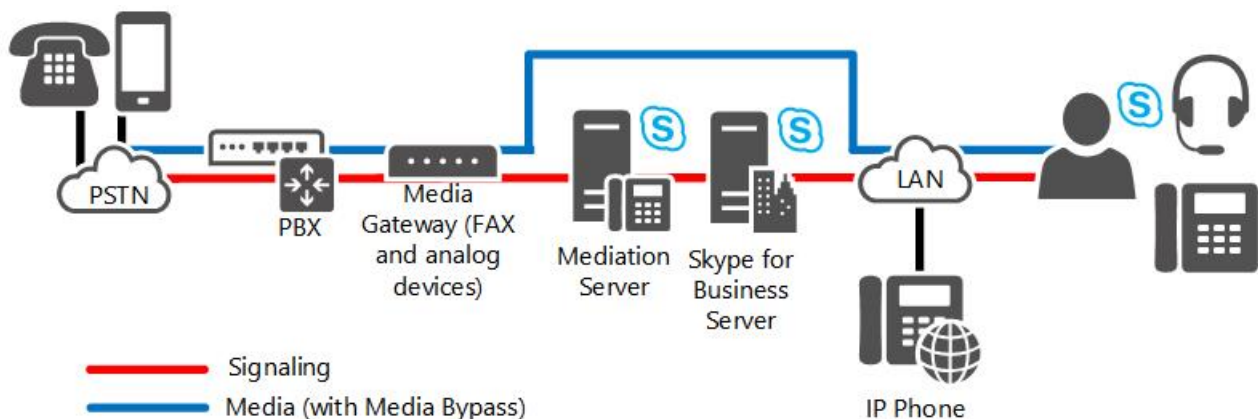
In this deployment, all calls are routed over the IP network. Calls to the PSTN are routed to the appropriate PSTN gateway. Skype for Business or Lync Phone Edition serves as a softphone. Remote call control is unavailable and unnecessary because there are no PBX phones for users to control. Voice mail and auto-attendant services are available through the optional deployment of Exchange Unified Messaging (UM).

#### NOTE

In addition to the network infrastructure that is required to support Skype for Business Server, a VoIP-only deployment can use a small, qualified gateway to support fax machines and analog devices.

The following figure shows a typical topology for a VoIP-only deployment.

### VoIP-only deployment option



#### NOTE

The media path shown in this figure has media bypass enabled (the recommended configuration). If you opt to disable media bypass, the media path is routed through the Mediation Server.

## PSTN Gateway deployment options

### PSTN Gateways

Public switched telephone network (PSTN) gateways are third-party hardware components that translate signaling and media between the Enterprise Voice infrastructure and the PSTN, either directly or through connection to SIP trunks. In either topology, the gateway terminates the PSTN. The gateway is isolated in its own subnet and is connected to the enterprise network through the Mediation Server.

An enterprise with multiple sites would typically deploy one or more gateways at each site. Branch sites can connect to the PSTN either through a gateway, or through a Survivable Branch Appliance, which combines gateway and servers in a single box. If branch sites use a gateway, both a Registrar and Mediation Server are required on site, unless the WAN link is resilient. One or more Mediation Servers, which are collocated on Front End Servers, can route calls for the one or more gateways at each site. We recommend that the Registrar, Mediation Server, and gateway required on site are deployed as a Survivable Branch Appliance.

Determining the number, size, and location of PSTN gateways is perhaps the most important and expensive decision you must make when planning your Enterprise Voice infrastructure.

Here are the main questions to consider. Keep in mind that the answers to these questions are all interdependent

- How many PSTN gateways are needed? The answer depends on the number of users, the anticipated number of simultaneous calls (traffic load), and the number of sites (each site needs one).
- What size should the gateways be? The answer depends on the number of users at the site and on the traffic load.
- Where should the gateways be located? The answer depends in part on the topology and in part on the geographic distribution of your organization.

You should also consider your gateway topology options (for details, see [Gateway Topologies](#) later in this topic).

#### **M:N Trunk Support**

The Mediation Servers can route calls through multiple gateways, Session Border Controllers (SBCs) provided by Internet telephony service providers, or a combination of the two. Additionally, multiple Mediation Servers in the pool can interact with multiple gateways. The logical route defined between a Mediation Server and gateway is called a trunk. When an internal user places a PSTN call, outbound routing logic on the Front End pool chooses which trunk to route over out of all possible combinations that may be available for routing that particular call. With DNS load balancing, if a call fails to reach a gateway due to an issue with a particular Mediation Server in the pool, the call will be retried to an alternate Mediation Server in the pool.

For details about planning for multiple gateways, see [M:N trunk in Skype for Business Server](#).

For details about other outbound routing enhancements, see [Call Routes](#).

#### **Gateway Topologies**

When you consider the fundamental questions of gateway deployment, follow these steps:

1. Count the sites at which you want to provide PSTN connectivity by using Enterprise Voice.
2. Estimate the traffic at each site (number of users and average number of calls per hour per user).
3. Deploy one or more gateways at each site to handle the anticipated traffic.

With this topology, calls among workers at each site and between sites are all routed over your intranet. Calls to the PSTN are routed over the enterprise IP network to the gateways that are closest to the location of the destination numbers. But what if your organization supports dozens or hundreds or even thousands of sites spread across one or more continents, as many financial institutions and other large enterprises do? In such cases, deploying a separate gateway at each site is not practical.

To address this issue, many large companies prefer to deploy one or a few large telephony central sites.

In this topology, several large gateways sufficient to accommodate the anticipated user load are deployed at each central site. All calls to users in the enterprise are forwarded by the company's telephone service provider to a central site. Routing logic at the central site determines whether the call should be routed over the intranet or to the PSTN.

#### **Gateway Location**

Gateway location may also determine the types of gateways that you choose and how they are configured. There are dozens of PSTN protocols, none of which is a worldwide standard. If all your gateways are located in a single country/region, this is not an issue, but if you locate gateways in several countries/regions, each must be configured according to the PSTN standards of that country/region. Moreover, gateways that are certified for operation in, for example, Canada, may not be certified in India, Brazil, or the European Union.

#### **Gateway Size and Number**

The PSTN gateways that most organizations will consider deploying range in size from 2 to as many as 960 ports. (There are even larger gateways, but these are used mainly by telephone service providers.) When estimating the number of ports your organization requires, use the following guidelines:

- Organizations with light telephony usage (one PSTN call per user per hour) should allocate one port for every 15 users. For example, if you have 20 users, you will require a gateway with two ports.
- Organizations with moderate telephony usage (two PSTN calls per user per hour) should allocate one port for every 10 users. For example, if you have 100 users, you will require a total of 10 ports allocated among one or more gateways.
- Organizations with heavy telephony usage (three or more PSTN calls per user per hour) should allocate one port for every five users. For example, if you have 47,000 users, you will require a total of 9,400 ports allocated among at least 10 large gateways.
- Additional ports can be acquired as the number of users or amount of traffic in your organization increases.

For any given number of users you must support, you have the choice of deploying fewer, larger gateways, or smaller ones. As a rule, a minimum of two gateways for an organization is recommended to maintain availability if one gateway fails.

Each PSTN gateway that you deploy must have at least one corresponding Mediation Server.

# M:N trunk in Skype for Business Server

5/20/2019 • 4 minutes to read

Skype for Business Server Enterprise Voice supports M:N trunking between Mediation Server and components such as PSTN gateways, session border controllers, and IP-PBX.

Skype for Business Server supports greater flexibility in the definition of a trunk for call routing purposes from previous releases. A trunk is a logical association between a Mediation Server and listening port number with a gateway and a listening port number. This implies several things: A Mediation Server can have multiple trunks to the same gateway; a Mediation Server can have multiple trunks to different gateways; conversely a gateway can have multiple trunks to different Mediation Servers.

You must still create a root trunk whenever you use Topology Builder to add a gateway to the topology. The number of gateways that a given Mediation Server can handle depends on the processing capacity of the server during peak busy hours. If you deploy a Mediation Server on hardware that exceeds the minimum hardware requirements for Skype for Business Server, as described in [Server requirements for Skype for Business Server 2015](#), then the estimate of how many active non-bypass calls a stand-alone Mediation Server can handle is approximately 1000 calls. When deployed on hardware meeting these specifications, the Mediation Server is expected to perform transcoding, but still route calls for multiple gateways even if the gateways do not support media bypass.

When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with that route. Instead, you use Topology Builder to associate trunks with Mediation Servers. In other words, routing determines which trunk to use for a call, and, subsequently, the Mediation Server associated with that trunk is sent the signaling for that call.

The Mediation Server can be deployed as a pool; this pool can be collocated with a Front End pool, or it can be deployed as a stand-alone pool. When a Mediation Server is collocated with a Front End pool, the pool size can be at most 12 (the limit of the Registrar pool size). Taken together, these new capabilities increase the reliability and deployment flexibility for Mediation Servers, but they require associated capabilities in the following peer entities:

- **PSTN gateway.** A Skype for Business Server qualified gateway must implement DNS load balancing, which enables a qualified public switched telephone network (PSTN) gateway to act as a load balancer for one pool of Mediation Servers, and thereby to load-balance calls across the pool.
- **Session Border Controller.** For a SIP trunk, the peer entity is a Session Border Controller (SBC) at an Internet telephony service provider. In the direction from the Mediation Server pool to the SBC, the SBC can receive connections from any Mediation Server in the pool. In the direction from the SBC to the pool, traffic can be sent to any Mediation Server in the pool. One method of achieving this is through DNS load balancing, if supported by the service provider and SBC. An alternative is to give the service provider the IP addresses of all Mediation Servers in the pool, and the service provider will provision these in their SBC as a separate SIP trunk for each Mediation Server. The service provider will then handle the load balancing for its own servers. Not all service providers or SBCs may support these capabilities. Furthermore, the service provider may charge extra for this capability. Typically, each SIP trunk to the SBC incurs a monthly fee.
- **IP-PBX.** In the direction from the Mediation Server pool to the IP-PBX SIP termination, the IP-PBX can receive connections from any Mediation Server in the pool. In the direction from the IP-PBX to the pool, traffic can be sent to any Mediation Server in the pool. Because most IP-PBXs do not support DNS load balancing, we recommend that individual direct SIP connections be defined from the IP-PBX to each Mediation Server in the pool. The IP-PBX will then handle its own load balancing by distributing traffic over the trunk group. The assumption is that the trunk group has a consistent set of routing rules at the IP-PBX.

Whether a particular IP-PBX supports this trunk group concept and how it intersects with the IP-PBX's own redundancy and clustering architecture needs to be determined before you can decide whether a Mediation Server cluster can interact correctly with an IP-PBX.

A Mediation Server pool must have a uniform view of the peer gateway with which it interacts. This means that all members of the pool access the same definition of the peer gateway from the configuration store and are equally likely to interact with it for outgoing calls. Therefore, there is no way to segment the pool so that some Mediation Servers communicate with only certain gateway peers for outgoing calls. If such segmentation is necessary, a separate pool of Mediation Servers must be used. This would be the case, for example, if the associated capabilities in PSTN gateways, SIP trunks, or IP-PBXs to interact with a pool as detailed earlier in this topic are not present.

A particular PSTN gateway, IP-PBX, or SIP trunk peer can route to multiple Mediation Servers or trunks. The number of gateways that a particular pool of Mediation Servers can control depends on the number of calls that use media bypass. If a large number of calls use media bypass, a Mediation Server in the pool can handle many more calls, because only signaling layer processing is necessary.

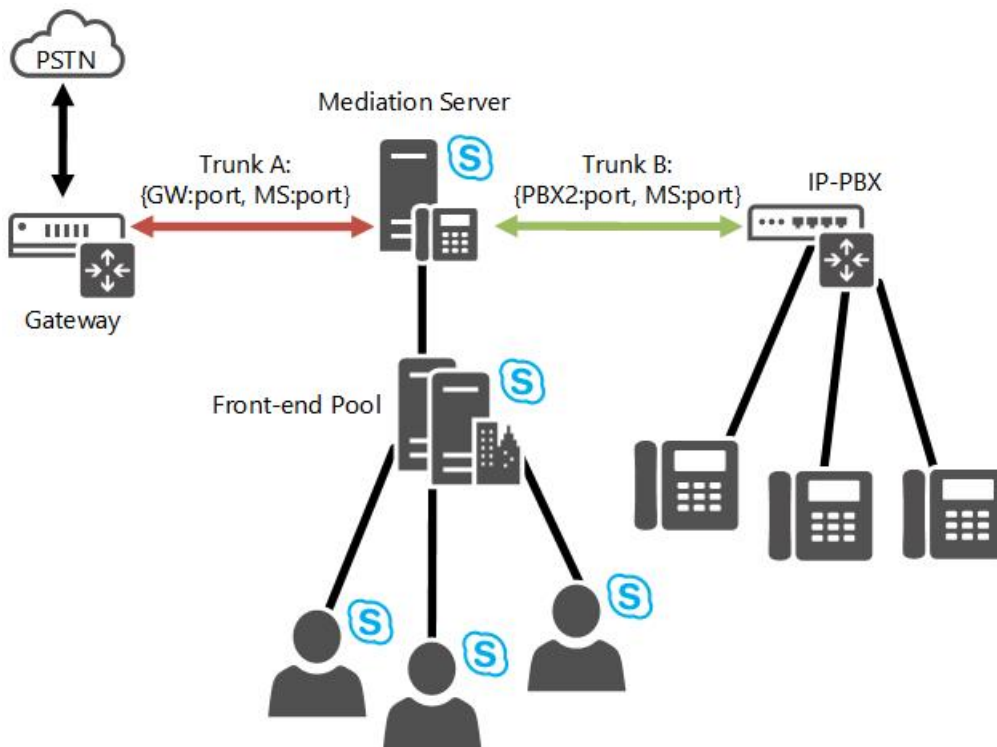
# Inter-trunk routing in Skype for Business Server

5/20/2019 • 2 minutes to read

Learn how Skype for Business Server Enterprise Voice supports inter-trunk routing.

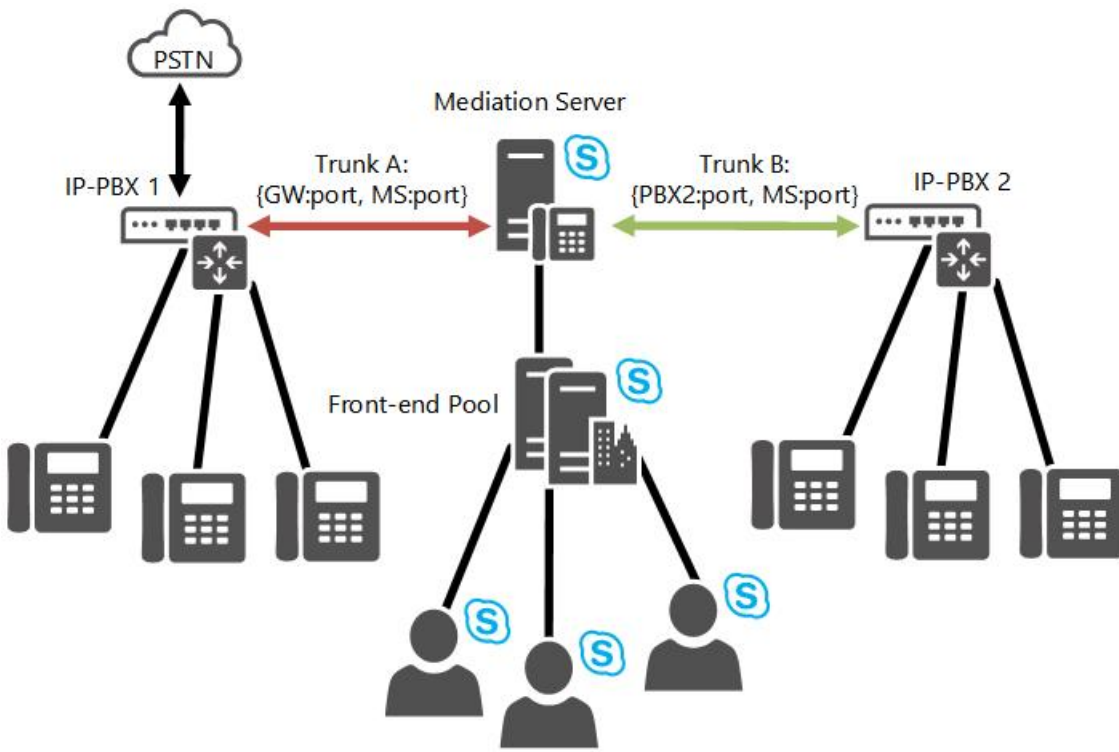
Skype for Business Server provides basic session management through the support of intertrunk routing. This enables Skype for Business Server to provide call control functionalities to downstream telephony systems. Intertrunk routing can interconnect an IP-PBX to a public switched telephone network (PSTN) gateway so that calls from a private branch exchange (PBX) phone can be routed to the PSTN, and incoming PSTN calls can be routed to a PBX phone. Similarly, Skype for Business Server can interconnect two or more IP-PBX systems so that calls can be placed and received between PBX phones from the different IP-PBX systems.

The following figure illustrates Skype for Business Server providing interconnectivity between a PSTN gateway and an IP-PBX.



The next figure illustrates Skype for Business Server connecting two IP-PBX systems.





# Translation rules in Skype for Business Server

5/20/2019 • 2 minutes to read

Learn about translation rules and dial string normalization in Skype for Business Server Enterprise Voice.

Enterprise Voice requires that all dial strings be normalized to E.164 format for the purpose of performing reverse number lookup (RNL). Translation rules are supported for both called numbers and calling numbers. The trunk peer (that is, the associated gateway, private branch exchange (PBX), or SIP trunk) may require that numbers be in a local dialing format. To translate numbers from E.164 format to a local dialing format, you can define one or more translation rules to manipulate the request URI before you route it to the trunk peer. For example, you could write a translation rule to remove +44 from the beginning of a dial string and replace it with 0144.

By performing outbound route translation on the server, you can reduce the configuration requirements on each individual trunk peer in order to translate phone numbers into a local dialing format. When you plan which gateways, and how many gateways, to associate with a specific Mediation Server cluster, it may be useful to group trunk peers with similar local dialing requirements. This can reduce the number of required translation rules and the time it takes to write them.

## IMPORTANT

Associating one or more translation rules with an Enterprise Voice trunk configuration should be used as an alternative to configuring translation rules on the trunk peer. Do not associate translation rules with an Enterprise Voice trunk configuration if you have configured translation rules on the trunk peer, because the two rules might conflict.

## Example Translation Rules

The following examples of translation rules show how you can develop rules on the server to translate numbers from E.164 format to a local format for the trunk peer.

For details about how to implement translation rules, see [Defining Translation Rules](#) in the Deployment documentation.

DESCRIPTION	STARTING DIGITS	LENGTH	DIGITS TO REMOVE	DIGITS TO ADD	MATCHING PATTERN	TRANSLATION	EXAMPLE
Conventional long-distance dialing in U.S. (strip out the '+')	+1	Exactly 12	1	0	^+(1\d{10})\$	\$1	+14255551010 becomes 14255551010
U.S. international long-distance dialing (strip out '+' and add 011)	+	At least 11	1	011	^+(\d{9})\d+\$	011\$1	+441235551010 becomes 011441235551010

# Plan for outbound voice routing in Skype for Business Server

5/20/2019 • 20 minutes to read

Learn about outbound voice routing in Skype for Business Server Enterprise Voice, including call routing settings, dial plans, normalization rules, voice policies, PSTN usage records, and voice routes.

Outbound call routing applies to Enterprise Voice calls that are destined for a public switched telephone network (PSTN) gateway, trunk, or private branch exchange (PBX). When a Skype for Business user places a call, the server normalizes the phone number to E.164 format, if necessary, and attempts to match it to a SIP URI. If the server cannot make the match, it applies outbound call routing logic based on the supplied dial string. You define that logic by configuring the server settings that are described in the following table.

## Skype for Business Server Outbound Call Routing Settings

OBJECT	DESCRIPTION
Dial Plan	A dial plan is a named set of normalization rules that translates phone numbers for a named location, individual user, or contact object into a single standard (E.164) format for purposes of phone authorization and call routing.
Normalization rule	Normalization rules define how phone numbers expressed in various formats are to be routed for each specified location, user, or contact object. The same dial string may be interpreted and translated differently, depending on the location from which it is dialed and the person or contact object that makes the call. A set of normalization rules associated with a particular location constitutes a dial plan.
Voice policy	A voice policy associates one or more PSTN usage records with one user or a group of users. A voice policy also provides a list of calling features that you can enable or disable.
PSTN usage record	A PSTN usage record specifies a class of call (such as internal, local, or long distance) that can be made by various users, or groups of users, in an organization.
Call Route	A call route associates destination phone numbers with particular trunks and PSTN usage records. A PSTN gateway is considered a trunk.

## Dial plans and normalization rules

A dial plan is a named set of normalization rules that translates phone numbers for a named location, individual user, or contact object into a single standard (E.164) format for purposes of phone authorization and call routing.

Normalization rules define how phone numbers expressed in various formats are to be routed for each specified location, user, or contact object. The same dial string may be interpreted and translated differently, depending on the location from which it is dialed and the person or contact object making the call.

### Dial Plan Scope

A dial plan's scope determines the hierarchical level at which the dial plan can be applied. In Skype for Business Server, a user can be assigned a specific per-user dial plan. If a user dial plan is not assigned, the Front End pool dial plan is applied. If there is no Front End pool dial plan, the site dial plan is applied. Finally, if there is no other dial plan applicable to the user, the global dial plan is applied.

Clients obtain dial plan scope levels through in-band provisioning settings that are provided when users log on to Skype for Business. As the administrator, you can manage and assign dial plan scope levels by using Skype for Business Server Control Panel.

#### NOTE

The service level public switched telephone network (PSTN) gateway dial plan is applied to the incoming calls from a particular gateway.

Dial plan scope levels are defined as follows:

- **User dial plan:** Can be assigned to individual users, groups, or contact objects. Voice applications can look up a per-user dial plan when a call is received with the phone-context set to user-default. For the purpose of assigning a dial plan, a contact object is treated as an individual user.
- **Pool dial plan:** Can be created at the service level for any PSTN gateway or Registrar in your topology. To define a pool dial plan, you must specify the particular service (PSTN gateway or Registrar pool) to which the dial plan applies.
- **Site dial plan:** Can be created for an entire site, except for any users, groups, or contact objects that are assigned a pool dial plan or user dial plan. To define a site dial plan, you must specify the site to which the dial plan applies.
- **Global dial plan:** The default dial plan installed with the product. You can edit the global dial plan, but you cannot delete it. This dial plan applies to all Enterprise Voice users, groups, and contact objects in your deployment, unless you configure and assign a dial plan with a more specific scope.

#### Planning for Dial Plans

To plan a dial plan, follow these steps:

- List all the locales in which your organization has an office.

The list must be up-to-date and complete. It will need to be revised as company organization evolves. In a large, multinational company with numerous small branch offices, this can be a time-consuming task.

- Identify valid number patterns for each site.

The most time-consuming part of planning your dial plans is identifying the valid number patterns for each site. In some cases, you may be able to copy normalization rules that you have written for one dial plan to other dial plans, especially if the corresponding sites are within the same country/region or even continent. In other cases, small changes to numbers in one dial plan may be enough to use them in other dial plans.

- Develop an organization-wide scheme for naming dial plans.

Adopting a standard naming scheme assures consistency across an organization and makes maintenance and updates easier.

- Decide whether multiple dial plans are required for a single location.

If your organization maintains a single dial plan across multiple locations, you may still need to create a separate dial plan for Enterprise Voice users who are migrating from a private branch exchange (PBX) and who need to have their existing extensions retained.

- Decide whether per-user dial plans are required. For example, if you have users at a branch site who are registered with the central site or if you have users who are registered on a Survivable Branch Appliance, you can consider special dialing scenarios for such users using per-user dial plans and normalization rules. For details, see [Plan for Enterprise Voice resiliency in Skype for Business Server](#).
- Determine dial plan scope (as previously described in this topic).

To create a dial plan, you specify values in the following fields, as required, by using Skype for Business Server Control Panel or Skype for Business Server Management Shell.

#### **Name and Simple Name**

For user dial plans, you should specify a descriptive name that identifies the users, groups, or contact objects to which the dial plan will be assigned. For site dial plans, the Name field is pre-populated with the site name and cannot be changed. For pool dial plans, the Name field is pre-populated with the PSTN gateway or Front End pool fully qualified domain name (FQDN) and cannot be changed.

The dial plan Simple Name is pre-populated with a string that is derived from the dial plan name. The Simple Name field is editable, which enables you to create a more descriptive naming convention for your dial plans. The Simple Name value cannot be empty and must be unique. A best practice is to develop a naming convention for your entire organization and then use this convention consistently across all sites and users.

#### **Description**

We recommend that you type the common, recognizable name of the geographic location to which the corresponding dial plan applies. For example, if the dial plan name is London.Contoso.com, the recommended description would be London.

#### **Dial-in Conferencing Region**

If you are deploying dial-in conferencing, you will need to specify a dial-in conferencing region to associate dial-in conferencing access numbers with a dial plan.

#### **External Access Prefix**

You can specify an external access prefix of up to four characters (#, \*, and 0-9) if users need to dial one or more additional leading digits (for example, 9) to get an external line.

#### **NOTE**

If you specify an external access prefix, you do not need to create an additional normalization rule to accommodate the prefix.

### **Normalization Rules**

Normalization rules define how phone numbers expressed in various formats are to be routed for the named location. The same number string may be interpreted and translated differently, depending on the locale from which it is dialed. Normalization rules are necessary for call routing because users can, and do, use various formats when entering phone numbers in their Contacts lists.

Normalizing user-supplied phone numbers provides a consistent format that facilitates the following tasks:

- Match a dialed number to the intended recipient's SIP-URI.
- Apply dialing authorization rules to the calling party.

The following number fields are among those that your normalization rules may need to account for:

- Dial plan
- Country code
- Area code

- Length of extension
- Site prefix

### Creating Normalization Rules

Normalization rules use .NET Framework regular expressions to specify numeric match patterns that the server uses to translate dial strings to E.164 format for the purpose of performing reverse number lookup. You create normalization rules in the Skype for Business Server Control Panel either by entering the expressions manually, or by entering the starting digits and the length of the dial strings to be matched and letting the Skype for Business Server Control Panel generate the corresponding regular expression for you. Either way, when you finish, you can enter a test number to verify that the normalization rule works as expected.

For details about using .NET Framework regular expressions, see "[.NET Framework Regular Expressions](#)".

### Sample Normalization Rules

The following table shows sample normalization rules that are written as .NET Framework regular expressions. The samples are examples only and are not meant to be a prescriptive reference for creating your own normalization rules.

**Table 1. Normalization Rules Using .NET Framework Regular Expressions**

RULE NAME	DESCRIPTION	NUMBER PATTERN	TRANSLATION	EXAMPLE
4digitExtension	Translates 4-digit extensions	^\d{4}\$	+1425555\$1	0100 is translated to +14255550100
5digitExtension	Translates 5-digit extensions	^5\d{4}\$	+1425555\$1	50100 is translated to +14255550100
7digitcallingRedmond	Translates 7-digit numbers to Redmond local numbers	^\d{7}\$	+1425\$1	5550100 is translated to +14255550100
7digitcallingDallas	Translates 7-digit numbers to Dallas local numbers	^\d{7}\$	+1972\$1	5550100 is translated to +19725550100
10digitcallingUS	Translates 10-digit numbers in the United States	^\d{10}\$	+1\$1	2065550100 is translated to +12065550100
LDCallingUS	Translates numbers with long distance prefixes in the United States	^1\d{10}\$	+\$1	12145550100 is translated to +2145550100
IntlCallingUS	Translates numbers with international prefixes in the United States	^011\d*\$	+\$1	01191445550100 is translated to +91445550100
RedmondOperator	Translates 0 to Redmond Operator	^0\$	+14255550100	0 is translated to +14255550100
RedmondSitePrefix	Translates numbers with on-net prefix (6) and Redmond site code (222)	^6222\d{4}\$	+1425555\$1	62220100 is translated to +14255550100

RULE NAME	DESCRIPTION	NUMBER PATTERN	TRANSLATION	EXAMPLE
NYSitePrefix	Translates numbers with on-net prefix (6) and NY site code (333)	^6333(\d{4})\$	+1202555\$1	63330100 is translated to +12025550100
DallasSitePrefix	Translates numbers with on-net prefix (6) and Dallas site code (444)	^6444(\d{4})\$	+1972555\$1	64440100 is translated to +19725550100

The following table illustrates a sample dial plan for Redmond, Washington, United States, based on the normalization rules shown in the previous table.

**Table 2. Redmond Dial Plan Based on Normalization Rules Shown in Table 1**

<b>REDMOND.FORESTFQDN</b>
5digitExtension
7digitcallingRedmond
10digitcallingUS
IntlCallingUS
RedmondSitePrefix
NYSitePrefix
DallasSitePrefix
RedmondOperator

**NOTE**

The normalization rules names shown in the preceding table do not include spaces, but this is a matter of choice. The first name in the table, for example, could have been written "5 digit extension" or "5-digit Extension" and still be valid.

## Voice policies

Skype for Business Server voice policies define the following for each user, site, or organization that is assigned the policy:

- A set of calling features that can be enabled or disabled to determine the Enterprise Voice functionality available to users.
- A set of public switched telephone network (PSTN) usage records that define what types of calls are authorized.

The following steps will help you plan the voice policies that you will need for your Enterprise Voice deployment:

- Determine how you will configure your global voice policy (the default voice policy that is installed with the product). This policy will apply to all Enterprise Voice users who are not explicitly assigned a site-level or

per-user policy.

- Identify any site-level voice policies that you might need.
- Identify any per-user voice policies that you might need.
- Decide which call features to enable for each voice policy.
- Determine what PSTN usage records to configure for each voice policy.

### Voice Policy Scope

Voice policy scope determines the hierarchical level at which the policy can be applied. In Skype for Business Server, you can configure voice policies with the following scope levels (listed from the most specific to the most general).

- **User voice policy** can be assigned to individual users, groups, or contact objects. This is the lowest level policy. User voice policies can be deployed to enable features for certain users or groups at a site, but not for others in the same site. For example, you may want to disable long distance dialing for some employees. For the purpose of assigning a voice policy, a contact object is treated as an individual user.

#### NOTE

We recommend that you deploy a user voice policy for branch site Enterprise Voice users who are registered with the central site deployment, or users who are registered on a Survivable Branch Appliance.

- **Site voice policy** applies to an entire site, except for any users, groups, or contact objects that are assigned a user voice policy. To define a site voice policy, you must specify the site to which the policy applies. If a user voice policy is not assigned, the site voice policy is used.
- **Global voice policy** is the default voice policy that is installed with the product. You can edit the global voice policy to meet the specific needs of your organization, but you cannot rename or delete it. This voice policy applies to all Enterprise Voice users, groups, and contact objects in your deployment unless you configure and assign a voice policy with more specific scope. If you want to disable this policy entirely, be sure that all sites and users have custom policies assigned to them.

### Call Features

You can enable or disable the following call features for each voice policy:

- **Call forwarding** enables users to forward calls to other phones and client devices. Enabled by default.
- **Delegation** enables users to specify other users to send and receive calls on their behalf. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on an additional phone (for example, a mobile phone) or other endpoint devices. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN reroute** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the public switched telephone network (PSTN) if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override call admission control policy decisions for



a particular user. Disabled by default.

- **Malicious call tracing** enables users to report malicious calls by using the Skype for Business client, and then flags such calls in the call detail records. Disabled by default.
- **Voicemail escape** prevents calls from being immediately routed to the user's mobile phone voicemail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range, and is based on a timer value. This setting enables and disables the timer and sets the value of the timer. It can be configured only by using the Skype for Business Server Management Shell. Disabled by default.
- **Call forwarding and simultaneous ringing PSTN usages** enables administrators to specify the same PSTN usage as the voice policy for call forwarding and simultaneous ringing, restrict call forwarding and simultaneous ringing to internal Skype for Business users only, or specify a custom PSTN usage that is different from the voice policy's PSTN usage. The default is to use the same PSTN usage as the voice policy for call forwarding and simultaneous ringing.

### PSTN Usage Records

Each voice policy should have one or more associated PSTN usage records. PSTN usages can be associated with a voice policy for the purpose of simultaneous ringing and call forwarding only.

#### NOTE

PSTN usage order is critical because in matching users to routes, the outbound routing functionality compares PSTN usages from top to bottom. If the first usage matches the call route, that route is used. If not, the outbound routing functionality looks at the next PSTN usage on the list and continues until a match is found. In effect, the subsequent PSTN usages provide backup if the first one on the list is unavailable.

## PSTN usage records

Planning PSTN usage records consists mainly of listing all the call permissions that are currently in force in your organization, from the CEO to temporary workers, consultants, and contingent staff. This process also provides an opportunity to reexamine existing call permissions and revise them. You can create PSTN usage records only for those call permissions that apply to your anticipated Enterprise Voice users, but a better long-range solution might be to create PSTN usage records for all call permissions, regardless of whether some may not currently apply to the group of users to be enabled for Enterprise Voice. If call permissions change or new users with different call permissions are added, you will have already created the required PSTN usage records.

The following table shows a typical PSTN usage table.

### PSTN Usage Records

PHONE ATTRIBUTE	DESCRIPTION
Local	Local calls
Long-Distance	Long distance calls
International	International calls
Delhi	Delhi full-time employees
Redmond	Redmond full-time employees
RedmondTemps	Redmond temporary employees

PHONE ATTRIBUTE	DESCRIPTION
Zurich	Zurich full-time employees

By themselves, PSTN usage records do not do anything. For them to work, you must associate them with the following:

- Voice policies, which are assigned to users.
- Routes, which are assigned to phone numbers.

## Voice routes

Call routes specify how Skype for Business Server handles outbound calls placed by Enterprise Voice users. When a user dials a number, the Front End Server normalizes the dial string to E.164 format, if necessary, and attempts to match it to a SIP URI. If the server cannot make the match, it applies outgoing call routing logic based on the number. The final step in defining that logic is to create a separate named call route for each set of destination phone numbers that are listed in each dial plan.

Before you define outbound call routes, you should complete the following steps:

- Deploy one or more trunks.
- Create dial plans as needed for sites, individuals, and Contact objects.
- Create public switched telephone network (PSTN) usage records.

Additionally, to enable outbound call routing, you must create and assign one or more voice policies. You can do this either before or after you define outbound call routes.

For each route, you must specify:

- A name by which the route can be easily identified.
- An optional description in cases where the name alone may not be sufficient to describe the route.
- The regular expression matching pattern that identifies the destination phone numbers to which the route is applied, along with exceptions to which the matching pattern is not to be applied.
- One or more trunks that you want to assign to the route.
- The PSTN usage records that users must have in order to call numbers matching the destination phone number regular expression.

You can specify call routes in the Skype for Business Server Control Panel. These call routes populate the server routing table, which Skype for Business Server uses to route calls that are destined for the PSTN.

### M:N Trunk Support

Skype for Business Server provides flexibility in how calls are routed to the PSTN. A voice route specifies a set of trunks to the PSTN that can be used for a particular voice call. A trunk associates a Mediation Server and a port number with a PSTN gateway and listening port number. This logical association enables a Mediation Server to be associated with multiple gateways and have multiple connections to the same gateway. When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with the route. To create trunks by defining the relationships between Mediation Servers and PSTN gateways, IP-PBXs, and Session Border Controllers (SBCs), use the Topology Builder.

### Least-Cost Routing

The ability to specify the trunks to which various numbers are routed enables you to determine which routes incur

the lowest costs and implement them accordingly. The general rule in selecting trunks is to choose the trunk with the closest gateway to the location of the destination number in order to minimize long-distance charges. For example, if you are in New York and calling a number in Rome, you would carry the call over the IP network to the trunk with the gateway in your Rome office, thereby incurring a charge only for a local call.

For an example of how least-cost routing might be used, consider the following: Fabrikam decides to enable German users to dial U.S. numbers by using the U.S. trunk. Fabrikam also wants to configure the system so that all calls from U.S. Skype for Business Server users to Germany and adjacent countries/regions terminate on the trunk with the gateway in Germany. This routing will save money, because a call from Germany to Austria, for example, is less expensive than a call from the U.S. to Austria.

### Translating Outbound Dial Strings

Skype for Business Server requires all dial strings to be normalized to E.164 format for the purpose of performing reverse number lookup (RNL). For trunks with gateways or private branch exchanges (PBXs) that require numbers translated in local dialing formats, Skype for Business Server enables you to create one or more rules that assist in manipulating the called number (i.e. Request URI) prior to routing it to the trunk. For example, you could write a rule to remove +44 from the head of a dial string and replace it with 0144.

With Skype for Business Server, it is possible to create one or more rules that assist in manipulating the calling number prior to routing it to the trunk.

In planning your trunks that associate gateway:port pairs with Mediation Server:port pairs, it may be useful to group trunks with similar local dialing requirements, and therefore reduce the number of required translation rules and the time it takes to write them.

### Configuring Caller ID

Skype for Business Server provides a way to manipulate the caller ID for outbound calls. For example, if an organization wants to mask employees' direct-dial extensions and replace them with the generic corporate or departmental number, an administrator can do that by using Skype for Business Server Control Panel to suppress the caller ID and replace it with a specified alternative caller ID. In planning your routing logic, consider which individuals, groups, sites you'll want this option for—perhaps, even, for all employees.

#### NOTE

For calls that are rerouted over the PSTN, the generic caller ID will be presented instead of the original caller ID. This can cause the call to bypass Do Not Disturb or privacy settings that the callee may have configured.

### Additional Routing Logic

In creating outbound call routes, you should be aware of the following factors that can affect routing logic:

- Where a call is established over a federated boundary, the domain portion of the URI is used to route the call over to the enterprise that is responsible for applying the outbound routing logic.
- If the domain portion of the request URI does not contain a supported domain for the enterprise, the outbound routing component on the server does not process the call.
- If a user is not enabled for Enterprise Voice, the server applies other routing logic, as appropriate.
- If a call is routed to a gateway that is fully occupied (all trunk lines are busy), the gateway rejects the call and the outbound routing logic redirects the call to the next-least-cost route. Give this careful consideration, because a gateway sized for a small office overseas (for example, Zurich) may actually carry a significant amount of nonlocal traffic for international calls to Switzerland. If the gateway is not correctly sized for this additional traffic, calls to Switzerland may be routed by way of a gateway in Germany, resulting in larger toll charges.

# Plan for Enterprise Voice resiliency in Skype for Business Server

5/20/2019 • 27 minutes to read

Learn how to support voice resiliency in Skype for Business Server Enterprise Voice, at both central sites and branch sites. Branch site options include deploying Survivable Branch Appliances or Survivable Branch Servers.

Voice resiliency refers to the ability of users to continue making and receiving calls if a central site that hosts Skype for Business Server becomes unavailable, whether through a wide area network (WAN) failure or another cause. If a central site fails, Enterprise Voice service must continue uninterrupted through seamless failover to a backup site. In the event of WAN failure, branch site calls must be redirected to a local PSTN gateway. This section discusses planning for voice resiliency in the event of central-site or WAN failure.

## Central site resiliency

Increasingly, enterprises have multiple sites spread across the globe. Maintaining emergency services, access to help desk, and the ability to conduct critical business tasks when a central site is out of service is essential for any Enterprise Voice resiliency solution. When a central site becomes unavailable, the following conditions must be met:

- Voice failover must be provided.
- Users who ordinarily register with the Front End pool at the central site must be able to register with an alternative Front End pool. This can be done by creating multiple DNS SRV records, each of which resolves to a Director pool or Front End pool in each of your central sites. You can adjust the priority and weights of the SRV records so that users who are served by that central site get the corresponding Director and Front End pool ahead of those in other SRV records.
- Calls to and from users located at other sites must be rerouted to the PSTN.

This topic describes the recommended solution for securing central site voice resiliency.

### Architecture and Topology

Planning for voice resiliency at a central site requires a basic understanding of the central role played by the Skype for Business Server Registrar in enabling voice failover. The Skype for Business Server Registrar is a service that enables client registration and authentication and provides routing services. It runs on all Standard Edition server, Front End Server, Director, or Survivable Branch Appliance. A Registrar pool consists of Registrar Services running on the Front End pool and residing at the same site. A Skype for Business client discovers the Front End pool through the following discovery mechanism:

1. DNS SRV record
2. Autodiscovery Web Service
3. DHCP option 120

After the Skype for Business client connects to the Front End pool, it is directed by the load balancer to one of the Front End Servers in the pool. That Front End Server, in turn, redirects the client to a preferred Registrar in the pool.

Each user enabled for Enterprise Voice is assigned to a particular Registrar pool, which becomes that user's primary Registrar pool. At a given site, hundreds or thousands of users typically share a single primary Registrar

pool. To account for the consumption of central site resources by any branch site users that rely on the central site for presence, conferencing, or failover, we recommend that you consider each branch site user as though the user were a user registered with the central site. There are currently no limits on the number of branch site users, including users registered with a Survivable Branch Appliance.

To assure voice resiliency in the event of a central site failure, the primary Registrar pool must have a single designated backup Registrar pool located at another site. The backup can be configured by using Topology Builder resiliency settings. Assuming a resilient WAN link between the two sites, users whose primary Registrar pool is no longer available are automatically directed to the backup Registrar pool.

The following steps describe the client discovery and registration process:

1. A client discovers Skype for Business Server through DNS SRV records. In Skype for Business Server, DNS SRV records can be configured to return more than one FQDN to the DNS SRV query. For example, if enterprise Contoso has three central sites (North America, Europe, and Asia-Pacific) and a Director pool at each central site, DNS SRV records can point to the Director pool FQDNs in each of the three locations. As long as the Director pool in one of the locations is available, the client can connect to the first hop Skype for Business Server.

#### NOTE

Using a Director pool is optional. A Front End pool can be used instead.

2. The Director pool informs the Skype for Business client about the user's primary Registrar pool and backup Registrar pool.
3. The Skype for Business client attempts to connect to the user's primary Registrar pool first. If the primary Registrar pool is available, the Registrar accepts the registration. If the primary Registrar pool is unavailable, the Skype for Business client attempts to connect to the backup Registrar pool. If the backup Registrar pool is available and has determined that the user's primary Registrar pool is unavailable (by detecting a lack of heartbeat for a specified failover interval) the backup Registrar pool accepts the user's registration. After the backup Registrar detects that the primary Registrar is again available, the backup Registrar pool will redirect failover clients to their primary pool.

### Requirements and Recommendations

The following requirements and recommendations for implementing central site voice resiliency are appropriate for most organizations:

- The sites in which the primary and backup Registrar pools reside should be connected by a resilient WAN link.
- Each central site must contain a Registrar pool consisting of one or more Registrars.
- Each Registrar pool must be load-balanced by using DNS load balancing, hardware load balancing, or both. For detailed information about planning your load balancing configuration, see [Load balancing requirements for Skype for Business](#).
- Each user must be assigned to a primary Registrar pool by using either the Skype for Business Server Management Shell **set-CsUser** cmdlet or the Skype for Business Server Control Panel.
- The primary Registrar pool must have a single backup Registrar pool located in a different central site.
- The primary Registrar pool must be configured to fail over to the backup Registrar pool. By default, the primary Registrar is set to fail over to the backup Registrar pool after an interval of 300 seconds. You can change this interval by using the Skype for Business Server Topology Builder.
- Configure a failover route. When configuring the route, specify a gateway that is located at a different site

from the gateway specified in the primary route.

- If the central site contained your primary management server and the site is likely to be down for an extended period, you will need to reinstall your management tools at the backup site; otherwise, you won't be able to change any management settings.

## Dependencies

Skype for Business Server depends on the following infrastructure and software components to assure voice resiliency:

COMPONENT	FUNCTIONAL
DNS	Resolving SRV records and A records for server-server and server-client connectivity
Exchange and Exchange Web Services (EWS)	Contact storage; calendar data
Exchange Unified Messaging and Exchange Web Services	Call logs, voice mail list, voice mail
DHCP Options 120	If DNS SRV is unavailable, the client will attempt to use DHCP Option 120 to discover the Registrar. For this to work, either a DHCP server must be configured or Skype for Business Server DHCP must be enabled.

## Survivable Voice Features

If the preceding requirements and recommendations have been implemented, the following voice features will be provided by the backup Registrar pool:

- Outbound PSTN calls
- Inbound PSTN calls, if the telephony service provider supports the ability to fail over to a backup site
- Enterprise calls between users at both the same site and between two different sites
- Basic call handling, including call hold, retrieval, and transfer
- Two-party instant messaging and sharing audio and video between users at the same site
- Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services, but only if both parties to call delegation, or all team members, are configured at the same site.
- Existing phones and clients continue to work.
- Call detail recording (CDR)
- Authentication and authorization

Depending on how they are configured, the following voice features may or may not work when a primary central site is out of service:

- Voice mail deposit and retrieval

If you want to make Exchange UM available when the primary central site is out of service, you must do one of the following:

- Change DNS SRV records so that the Exchange UM servers at the central site point to backup Exchange UM servers at another site.
- Configure each user's Exchange UM dial plan to include Exchange UM servers at both the central site and the backup site, but designate the backup Exchange UM servers as disabled. If the primary

site becomes unavailable, the Exchange administrator has to mark the Exchange UM servers at the backup site as enabled.

If neither of the preceding solutions is possible, then Exchange UM will not be available in the event the central site becomes unavailable.

- Conferencing of all types

A user who has failed over to a backup site can join a conference that is created or hosted by an organizer whose pool is available but cannot create or host a conference on his or her own primary pool, which is no longer available. Similarly, others users cannot join conferences that are hosted on the affected user's primary pool.

The following voice features do not work when a primary central site is out of service:

- Conference Auto-Attendant
- Presence and DND-based routing
- Updating call forwarding settings
- Response Group service and Call Park
- Provisioning new phones and clients
- Address Book Web Search

## Branch site resiliency

If you want to provide branch-site resiliency, that is, high-availability Enterprise Voice service, you have three options for doing so:

- Survivable Branch Appliance
- Survivable Branch Server
- A full Skype for Business Server deployment at the branch site

This guide will help you evaluate which resiliency solution is best for your organization and, based on your resiliency solution, which PSTN-connectivity solution to use. It will also help you prepare to deploy the solution that you choose by describing prerequisites and other planning considerations.

### **Branch site resiliency features**

If you provide branch-site resiliency, if a branch site's WAN connection to a central site fails or if the central site is unreachable, the following voice features should continue to be available:

- Inbound and outbound public switched telephone network (PSTN) calls
- Enterprise calls between users at both the same site and between two different sites
- Basic call handling, including call hold, retrieval, and transfer
- Two-party instant messaging
- Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services, but only if the delegator and delegate (for example, a manager and the manager's administrator), or all team members, are configured at the same site
- Call detail records (CDRs)
- PSTN dial-in conferencing with Conferencing Auto-Attendant

- Voice mail capabilities, if you configure voice mail rerouting settings.
- User authentication and authorization

The following features will be available only if your resiliency solution is a full-scale Skype for Business Server deployment at the branch site:

- IM, web, and A/V conferencing
- Presence and Do Not Disturb (DND)-based routing (where calls are prevented from ringing on extensions that have DND activated)
- Updating call forwarding settings
- Response Group application and Call Park application
- Provisioning new phones and clients, but only if Active Directory Domain Services is present at the branch site.
- Enhanced 9-1-1 (E9-1-1)

If E9-1-1 is deployed, and the SIP trunk at the central site is not available because the WAN link is down, then the Survivable Branch Appliance will route E9-1-1 calls to the local branch gateway. To enable this feature, the branch-site users' voice policies should route calls to the local gateway in the event of WAN failure.

**NOTE**

SBA (survivable branch office) is not supported for XMPP. Users homed in a SBA configurations will not be able to send IMs or see Presence with XMPP contacts.

**Branch site resiliency solutions**

There are obvious advantages to providing branch-site resiliency to your organization. Specifically, if you lose the connection to the central site, branch site users will continue to have Enterprise Voice service and voice mail (if you configure voice mail rerouting settings). However, for sites with fewer than 25 users, a resiliency solution may not provide a sufficient return on investment.

If you decide to provide branch-site resiliency, you have three options. The following table can help you determine the best option for your organization.

IF YOU...	WE RECOMMEND THAT YOU USE A...
-----------	--------------------------------

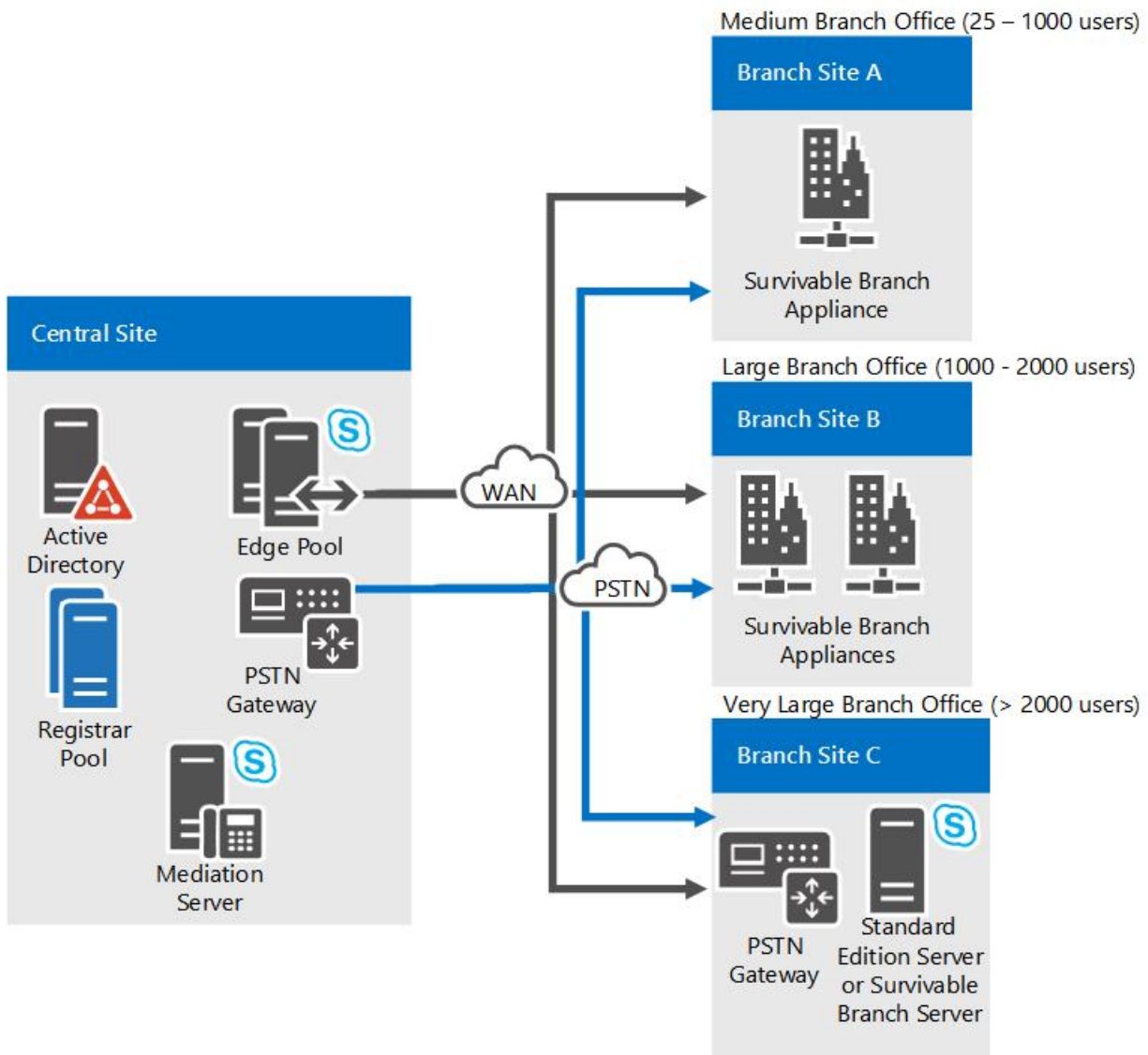


IF YOU...	WE RECOMMEND THAT YOU USE A...
<p>Host between 25 and 1000 users at your branch site, and if the return on investment does not support a full deployment or where local administrative support is unavailable</p>	<p>Survivable Branch Appliance</p> <p>The Survivable Branch Appliance is an industry-standard blade server with a Skype for Business Server Registrar and Mediation Server running on Windows Server 2008 R2. The Survivable Branch Appliance also contains a public switched telephone network (PSTN) gateway. Qualified third-party devices (developed by Microsoft partners in the Survivable Branch Appliance (SBA) qualification/certification program) provide a continuous PSTN connection in the event of WAN failure, but this approach does not provide resilient presence and conferencing because these features depend on Front End Servers at the central site.</p> <p>For details about Survivable Branch Appliances, see "Survivable Branch Appliance Details," later in this topic.</p> <p><b>Note:</b> If you decide to also use a SIP trunk with your Survivable Branch Appliance, contact your Survivable Branch Appliance vendor to learn about which service provider is best for your organization.</p>
<p>Host between 1000 and 2000 users at your branch site, lack a resilient WAN connection, and have trained Skype for Business Server administrators available</p>	<p>Survivable Branch Server or two Survivable Branch Appliances.</p> <p>The Survivable Branch Server is a Windows Server meeting specified hardware requirements that has Skype for Business Server Registrar and Mediation Server software installed on it. It must connect to either a PSTN gateway or a SIP trunk to a telephone service provider.</p> <p>For details about Survivable Branch Servers, see "Survivable Branch Server Details," later in this topic.</p>
<p>If you require presence and conferencing features in addition to voice features for up to 5000 users, and have trained Skype for Business Server administrators available</p>	<p>Deploy as a central site with a Standard Edition server rather than as a branch site.</p> <p>A full-scale Skype for Business Server deployment provides a continuous PSTN connection and resilient presence and conferencing in the event of WAN failure.</p>

### Resiliency Topologies

The following figure shows the recommended topologies for branch-site resiliency.

#### Branch site resiliency options



#### Survivable Branch Appliance Details

The Skype for Business Server Survivable Branch Appliance includes the following components:

- A Registrar for user authentication, registration and call routing
- A Mediation Server for handling signaling between the Registrar and a PSTN gateway
- A PSTN gateway for routing calls to the PSTN as a fallback transport in the event of a WAN outage
- SQL Server Express for local user data storage

The Survivable Branch Appliance also includes PSTN trunks, analog ports, and an Ethernet adapter.

If the branch site's WAN connection to a central site becomes unavailable, internal branch users continue to be registered with the Survivable Branch Appliance Registrar and obtain uninterrupted voice service by using the Survivable Branch Appliance connection to the PSTN. Branch site users who connect from home or other remote locations will be able to register with a Registrar server at a central site if the WAN link to the branch site is unavailable. These users will have full unified communications functionality, with the one exception that inbound calls to the branch site will go to voice mail. When the WAN connection becomes available, full functionality should be restored to branch site users. Neither the failover to the Survivable Branch Appliance nor the restoration of service requires the presence of an IT administrator.

Skype for Business Server supports up to two Survivable Branch Appliance at a branch site.

#### Survivable Branch Appliance Deployment Overview

The Survivable Branch Appliance is manufactured by original equipment manufacturers in partnership with

Microsoft and deployed on their behalf by value-added retailers. This deployment should occur only after Skype for Business Server has been deployed at the central site, a WAN connection to the branch site is in place, and branch site users are enabled for Enterprise Voice.

For details about these phases, see [Deploying a Survivable Branch Appliance or Server](#) in the Deployment documentation.

PHASE	STEPS	USER RIGHTS
Set up Active Directory Domain Services for the Survivable Branch Appliance	<p><b>At the central site:</b></p> <p>Create a domain user account (or enterprise identity) for the technician who will install and activate the Survivable Branch Appliance at the branch site.</p> <p>Create a computer account (with the applicable fully qualified domain name (FQDN)) for Survivable Branch Appliance in Active Directory Domain Services.</p> <p>In Topology Builder, create and publish the Survivable Branch Appliance.</p>	The technician user account must be a member of RTCUniversalSBATechnicians. The Survivable Branch Appliance must belong to the RTCUniversalServices group, which happens automatically when you use Topology Builder.
Install, and activate the Survivable Branch Appliance.	<p><b>At the branch site:</b></p> <p>Connect the Survivable Branch Appliance to an Ethernet port and PSTN port.</p> <p>Start the Survivable Branch Appliance.</p> <p>Join the Survivable Branch Appliance to the domain, using the domain user account created for the Survivable Branch Appliance at the central site. Set the FQDN and IP address to match the FQDN created in the computer account.</p> <p>Configure the Survivable Branch Appliance using the OEM user interface.</p> <p>Test PSTN connectivity.</p>	The technician user account must be a member of RTCUniversalSBATechnicians.

### Survivable Branch Server Details

In Topology Builder create the branch site, add the Survivable Branch Server to that site, and then run the Skype for Business Server Deployment Wizard on the computer where you want to install the role.

### Branch site resiliency requirements

This topic will help you to prepare users for branch-site resiliency and voice mail survivability, and also specifies the relevant hardware and software requirements.

#### Preparing Branch Users for Branch-Site Resiliency

Prepare users for branch-site resiliency by setting their Registrar pool as the Survivable Branch Appliance (SBA) or Survivable Branch Server.

#### Registrar Assignments for Branch Users

Regardless of which branch-site resiliency solution you choose, you will need to assign a primary Registrar to each user. Branch site users should always register with the Registrar at the branch site, regardless of whether that Registrar resides in the Survivable Branch Appliance, Survivable Branch Server, or stand-alone Skype for Business Server Standard or Enterprise Edition server. A domain name system (DNS) service (SRV) resource record is required so that a client can discover its Registrar pool. If the Survivable Branch Appliance becomes unavailable, this is how branch site clients will automatically discover the backup Registrar.

If a branch site does not have a DNS server, there are two alternative ways to configure discovery of the Survivable Branch Appliance or Survivable Branch Server:

- Configure DHCP option 120 on the branch site's Dynamic Host Configuration Protocol (DHCP) server to point to the fully qualified domain name (FQDN) of the Survivable Branch Appliance or Survivable Branch Server.
- Configure the Survivable Branch Appliance or Survivable Branch Server to respond to DHCP 120 queries.

#### Voice Routing for Branch Users

We recommend that you create a separate user-level Voice over Internet Protocol (VoIP) policy for users in a branch site. This policy should include a primary route that uses the Survivable Branch Appliance or branch server gateway, and one or more backup routes that use a trunk with a public switched telephone network (PSTN) gateway at the central site. If the primary route is unavailable, the backup route that uses one or more central site gateways is used instead. This way, regardless of where a user is registered—on the branch site Registrar or the backup Registrar pool at the central site—the user's VoIP policy is always in effect. This is an important consideration for failover scenarios. For example, if you need to rename the Survivable Branch Appliance or reconfigure the Survivable Branch Appliance to connect to a backup Registrar pool at the central site, then you must move branch site users to the central site for the duration. (For details about renaming or reconfiguring a Survivable Branch Appliance, see [Appendix B: Managing a Survivable Branch Appliance](#) in the Deployment documentation.) If those users do not have user-level VoIP policies or user-level dial plans, when the users are moved to another site, the site-level VoIP policies and site-level dial plans of the central site apply to the users by default, instead of the branch site site-level VoIP policies and dial plans. In this scenario, unless the site-level VoIP policies and site-level dial plans used by the backup Registrar pool can also apply to the branch site users, their calls will fail. For example, if users from a branch site located in Japan are moved to a central site in Redmond, then a dial plan with normalization rules that prepend +1425 to all 7-digit calls is unlikely to appropriately translate calls for those users.

#### IMPORTANT

When you create a branch office backup route, we recommend that you add two PSTN phone usage records to the branch office user policy and assign separate routes to each one. The first, or primary, route would direct calls to the gateway associated with the Survivable Branch Appliance (SBA) or branch server; the second, or backup, route would direct calls to the gateway at the central site. In directing calls, the SBA or branch server will attempt all routes assigned to the first PSTN usage record before attempting the second usage record.

To help ensure that inbound calls to branch site users will reach those users when the branch gateway or the Windows component of the Survivable Branch Appliance site is unavailable (which would happen, for example, if the Survivable Branch Appliance or branch gateway were down for maintenance), create a failover route on the gateway (or work with your Direct Inward Dialing (DID) provider) to redirect incoming calls to the backup Registrar pool at the central site. From there, the calls will be routed over the WAN link to branch users. Be sure that the route translates numbers to comply with the PSTN gateway or other trunk peer's accepted phone number formats. For details about creating a failover route, see [Configuring a Failover Route](#). Also create service-level dial plans for the trunk associated with the gateway at the branch site to normalize incoming calls. If you have two Survivable Branch Appliances at a branch site, you can create a site-level dial plan for both unless a separate service-level plan for each is necessary.

#### NOTE

To account for the consumption of central site resources by any branch site users that rely on the central site for presence, conferencing, or failover, we recommend that you consider each branch site user as if the user were registered with the central site. There are currently no limits on the number of branch site users, including users registered with a Survivable Branch Appliance.

We also recommend that you create a user-level dial plan and voice policy, and then assign it to branch site users. For details, see [Create or modify a dial plan in Skype for Business Server](#) and [Create the VoIP Routing Policy for Branch Users](#) in the Deployment documentation.

### Routing Extension Numbers

When preparing dial plans and voice policies for branch site users, be sure to include normalization rules and translation rules that match the strings and number format used in the msRTCSIP-line (or Line URI) attribute, so that Skype for Business calls enabled between branch site users and central site users will be routed correctly—particularly when calls must be rerouted over the PSTN because the WAN link is unavailable. Additionally, there are special considerations for dialed numbers that include extension numbers, rather just phone numbers.

Normalization rules and translations rules that match Line URIs that contain an extension number, whether exclusively or in addition to a full E.164 phone number, have additional requirements. This section describes several example scenarios to route calls for Line URIs with an extension number.

If your organization does not have Direct Inward Dial (DID) phone numbers configured for individual users and the Line URI of each user is configured with only an extension number, internal users can call one another by dialing only an extension number. However, you must configure normalization rules that can apply to calls from a branch site user to a central site user, that match the extension numbers.

In a scenario where the WAN link between a branch site and a central site is available, calls from branch site users to central site users do not require the matching normalization rule to translate the number because the call is not routed over the PSTN. For example:

RULE NAME	DESCRIPTION	NUMBER PATTERN	TRANSLATION	EXAMPLE
5digitExtensions	Does not translate 5-digit numbers	^\d{5}\$	\$1	10001 is not translated

You must also accommodate extension numbers for specific scenarios, such as when the WAN link between a branch site and central site is unavailable and a call from a branch site must be routed over the PSTN. During a WAN outage, if a branch site user calls a central site user only by dialing the central site user's extension, you must have an outbound translation rule that adds the central site user's full phone number. If a user's Line URI contains your organization's full phone number and the user's unique extension number instead of a full phone number that is unique to the user, then you must have an outbound translation rule that adds your organization's full phone number instead. For example:

DESCRIPTION	MATCHING PATTERN	TRANSLATION	EXAMPLE
Translates 5-digit numbers to a user's phone number and extension	^\d{5}\$	+14255550123;ext=\$1	10001 is translated to +14255550123;ext=10001
Translates 5-digit numbers to your organization's phone number and a user's extension	^\d{5}\$	+14255550100;ext=\$1	10001 is translated to +14255550100;ext=10001

In this scenario, if the trunk peer that handles rerouting to the PSTN does not support extension numbers, then the outbound translation rule must also remove the extension number. For example:

DESCRIPTION	MATCHING PATTERN	TRANSLATION	EXAMPLE
Removes extension from phone numbers with extensions	^+(\d*);ext=(\d*)\$	+\$1	+14255550123;ext=10001 is translated to +14255550123

Whether or not a WAN link is available, if your organization does not have DID numbers configured for individual users and the Line URI for a user contains your organization's phone number and the user's unique extension number, then you must configure your organization's phone number Line URI with a number that is reachable by the trunk peer or PSTN gateway at the branch site. You must also configure your organization's phone number Line URI to include its own unique extension for calls to be routed to that number.

#### **Preparing for Voice Mail Survivability**

Exchange Unified Messaging (UM) is usually installed only at a central site and not at branch sites. A caller should be able to leave a voice mail message, even if the WAN link between branch site and central site is unavailable. As a result, configuring the Line URI for the Exchange UM Auto Attendant phone number that provides voice mail for branch site users requires special considerations, in addition to the voice policy, dial plan, and normalization rules applicable to that voice mail number.

Survivable Branch Appliances (SBAs) and Survivable Branch Servers provide voice mail survivability for branch users during a WAN outage. Specifically, if you are using a Survivable Branch Appliance or Survivable Branch Server and the WAN becomes unavailable, the SBA or Survivable Branch Server reroutes unanswered calls over the PSTN to Exchange UM at the central site. With a SBA or Survivable Branch Server, users can also retrieve voice mail messages through the PSTN during a WAN outage. Finally, during a WAN outage the Survivable Branch Appliance or Survivable Branch Server queues missed-call notifications and then uploads them to the Exchange UM server when the WAN is restored. To help ensure that voice mail rerouting is resilient, be sure that you add an entry for the central site pool's FQDN and an entry for the Edge Server FQDN to the hosts file on the Survivable Branch Server. Otherwise, DNS resolution can time out if you do not have a DNS server at the branch site.

We recommend the following configurations for voice mail survivability for branch site users:

- An Microsoft Exchange administrator should configure Exchange UM Auto Attendant (AA) to accept messages only. This configuration disables all other generic functionality, such as transfer to a user or transfer to an operator, and limits the AA to only accepting messages. Alternatively, the Exchange administrator can use a generic AA or an AA customized to route the call to an operator.
- The Skype for Business Server administrator should take the AA phone number and use that phone number as the **exchange um auto attendant** number in the voice mail rerouting settings for the Survivable Branch Appliance or branch server.
- The Skype for Business Server administrator should get the Exchange UM subscriber access phone number and use that number as the **subscriber access** number in the voice mail rerouting settings for the Survivable Branch Appliance or Survivable Branch Server.
- The Skype for Business Server administrator should configure Exchange UM so that only one dial plan is associated with all branch users who need access to voice mail during a WAN outage.
- When the WAN link is unavailable, calls to branch site users can be routed to the user's Exchange Unified Messaging (UM) voice mailbox, but only if the voice policy applied to the call specifies a voice mail phone number that is unique and does not include an extension number.

#### **Hardware and Software Requirements for Branch-Site Resiliency**

The hardware and software requirements vary, depending on your resiliency solution.

##### **Requirements for Survivable Branch Appliances**

Required hardware and software is built into the Survivable Branch Appliance. However, we also recommend that each branch site deploy a DHCP server to obtain client IP addresses; otherwise, when the DHCP lease expires, clients will not have IP connectivity.

If the enterprise DNS servers are located only in central sites, branch site users will be unable to connect to them during a WAN outage, and therefore Skype for Business Server discovery that uses DNS SRV (service (SRV) resource record) will fail. To assure prompt rerouting during a WAN outage, DNS records must be cached at the

branch site. If the branch router supports it, turn on DNS caching. Or, you can deploy a DNS server at the branch. This can be a stand-alone server or a version of the Survivable Branch Appliance that supports DNS capabilities. For details, contact your Survivable Branch Appliance provider.

**NOTE**

It is not necessary to have a domain controller at a branch site. The Survivable Branch Appliance authenticates clients by using a special certificate that it sends the client in response to the client's certificate request when it signs in.

Skype for Business clients can discover the Skype for Business Server by using DHCP Option 120 (SIP Registrar Option). This can be configured in one of two ways:

- Configure the DHCP server at the branch site to reply to DHCP 120 queries, which return the FQDN of the Registrar on the Survivable Branch Appliance or Survivable Branch Server.
- Turn on Skype for Business Server DHCP. When this is turned on, the Skype for Business Server Registrar responds to DHCP Option 120 queries. Note that the Registrar does not respond to any DHCP queries other than DHCP Options 120.

Additionally, for larger branch sites that have multiple subnets, DHCP relay agents should be enabled to forward DHCP Option 120 queries to the DHCP Server (configuration 1) or to the Registrar (configuration 2).

Finally, branch site users must be configured for Enterprise Voice and provisioned with an appropriate unified communications endpoint.

**Requirements for Survivable Branch Servers**

The requirements for Survivable Branch Servers are the same as the requirements for a Front End Server. For details, see [Server requirements for Skype for Business Server 2015](#).

**Requirements for Full-Scale Skype for Business Server Branch-Site Deployments**

For details, see [Server requirements for Skype for Business Server 2015](#) in the Planning documentation.

**Example: configuring a failover route**

The following example shows how an administrator can define a failover route for use if the Dallas-GW1 is down for maintenance or is otherwise unavailable. The following tables illustrate the required configuration change.

**Table 1. User Policy**

USER POLICY	PHONE USAGE
Default Calling Policy	Local GlobalPSTNHopoff
Redmond Local Policy	RedmondLocal
Dallas Calling Policy	DallasUsers GlobalPSTNHopoff

**Table 2. Routes**

ROUTE NAME	NUMBER PATTERN	PHONE USAGE	TRUNK	GATEWAY
Redmond Local Route	^+1(425	206	253)(\d{7})\$	Local RedmondLocal
Dallas Local Route	^+1(972	214	469)(\d{7})\$	Local

<b>ROUTE NAME</b>	<b>NUMBER PATTERN</b>	<b>PHONE USAGE</b>	<b>TRUNK</b>	<b>GATEWAY</b>
Universal Route	^+?(\d*)\$	GlobalPSTNHopoff	Trunk1 Trunk2 Trunk3	Red-GW1 Red-GW2 Dallas-GW1
Dallas Users Route	^+?(\d*)\$	DallasUsers	Trunk3	Dallas-GW1

In Table 1, a phone usage of GlobalPSTNHopoff is added after the DallasUsers phone usage in the Dallas Calling Policy. This enables calls with the Dallas Calling policy to use routes that are configured for the GlobalPSTNHopoff phone usage if a route for the DallasUsers phone usage is unavailable.



# Network settings for the advanced Enterprise Voice features in Skype for Business Server

5/20/2019 • 5 minutes to read

Learn about network regions, network sites, and IP subnets. All these must be configured to deploy [Plan for media bypass in Skype for Business](#), [Plan for call admission control in Skype for Business Server](#), or [Plan for emergency services in Skype for Business Server](#) in Skype for Business Server Enterprise Voice.

Skype for Business Server has three advanced Enterprise Voice features: [Plan for call admission control in Skype for Business Server](#), [Plan for emergency services in Skype for Business Server](#), and [Plan for media bypass in Skype for Business](#). These features share certain configuration requirements for network regions, network sites, and association of each subnet in the Skype for Business Server topology with a network site.

This topic provides an overview of the configuration requirements that are common to all three of these advanced Enterprise Voice features.

## Network Regions

A network region is a network hub or network backbone used only in the configuration of call admission control (CAC), E9-1-1, and media bypass.

### NOTE

Network regions are not the same as Skype for Business Server dial-in conferencing regions, which are required to associate dial-in conferencing access numbers with one or more Skype for Business Server dial plans. For details about dial-in conferencing regions, see [Planning for Dial-In Conferencing](#).

CAC requires that every network region have an associated Skype for Business Server central site, which manages media traffic within the region (that is, it makes decisions based on policies that you have configured, regarding whether or not a real-time audio or video session can be established). Skype for Business Server central sites do not represent geographical locations, but rather logical groups of servers that are configured as a pool or a set of pools.

To configure a network region, you can either use the **Regions** tab on the **Network Configuration** section of Skype for Business Server Control Panel, or run the **New-CsNetworkRegion** or **Set-CsNetworkRegion** Skype for Business Server Management Shell cmdlets. For instructions, see [Deploy network regions, sites and subnets in Skype for Business](#) in the Deployment documentation, or refer to the Skype for Business Server Management Shell documentation.

The same network region definitions are shared by all three advanced Enterprise Voice features. If you have already created network regions for one feature, you do not need to create new network regions for the other features. You may, however, need to modify an existing network region definition to apply feature-specific settings. For example, if you have created network regions for E9-1-1 (which do not require an associated central site) and, later, you deploy call admission control, you must modify each of the network region definitions to specify a central site.

To associate a Skype for Business Server central site with a network region, you specify the central site name, either by using the **Network Configuration** section of Skype for Business Server Control Panel, or by running the **New-CsNetworkRegion** or **Set-CsNetworkRegion** cmdlets. For instructions, see [Deploy network regions, sites and subnets in Skype for Business](#) in the Deployment documentation, or refer to the Skype for Business

## Network Sites

A network site represents a geographical location, such as a branch office, a regional office, or a main office. Each network site must be associated with a specific network region.

### NOTE

Network sites are used only by the advanced Enterprise Voice features. They are not the same as the branch sites that you configure in your Skype for Business Server topology.

To configure a network site and associate it with a network region, you can either use the **Network Configuration** section of Skype for Business Server Control Panel, or run the Skype for Business Server Management Shell **New-CsNetworkSite** or **Set-CsNetworkSite** cmdlets. For details, see [Create or Modify a Network Site](#) in the Deployment documentation, or refer to the Skype for Business Server Management Shell documentation.

## Identify IP Subnets

For each network site, you will need to work with your network administrator to determine which IP subnets are assigned to each network site. If your network administrator has already organized the IP subnets into network regions and network sites, then your work is significantly simplified.

For example, the New York site in the North America region can be assigned the following IP subnets: 172.29.80.0/23, 157.57.216.0/25, 172.29.91.0/23, 172.29.81.0/24. If Bob, who usually works in Detroit, travels to the New York office for training, turns on his computer and connects to the network, his computer will get an IP address in one of the four ranges that are allocated for New York—for example, 172.29.80.103.

### Caution

The IP subnets specified during network configuration on the server must match the format that is provided by client computers in order to be properly used for media bypass. A Skype for Business client takes its local IP address and masks the IP address with the associated subnet mask. When determining the bypass ID associated with each client, the Registrar will compare the list of IP subnets associated with each network site against the subnet that is provided by the client for an exact match. For this reason, it is important that subnets entered during network configuration on the server are actual subnets instead of virtual subnets. (If you deploy call admission control, but not media bypass, call admission control will function properly even if you configure virtual subnets.) For example, if a Skype for Business client signs in on a computer with an IP address of 172.29.81.57 with an IP subnet mask of 255.255.255.0, it will request the bypass ID that is associated with subnet 172.29.81.0. If the subnet is defined as 172.29.0.0/16, although the client belongs to the virtual subnet, the Registrar will not consider this a match because the Registrar is specifically looking for subnet 172.29.81.0. Therefore, it is important that the administrator enters subnets exactly as provided by Skype for Business clients (which are provisioned with subnets during network configuration, either statically or by Dynamic Host Configuration Protocol (DHCP).)

## Associating Subnets with Network Sites

Every subnet in the enterprise network must be associated with a network site (that is, every subnet needs to be associated with a geographic location). This association of subnets enables the advanced Enterprise Voice features to locate the endpoints geographically. For example, locating the endpoints enables CAC to regulate the flow of real-time audio and video data going to and from the network site.

To associate subnets with network sites, you can either use the **Network Configuration** section of Skype for Business Server Control Panel, or you can use the Skype for Business Server Management Shell. For instructions, see [Associate a Subnet with a Network Site](#) in the Deployment documentation, or refer to the Skype for Business

Server Management Shell documentation.

## See also

[Plan for call admission control in Skype for Business Server](#)

[Plan for emergency services in Skype for Business Server](#)

[Plan for media bypass in Skype for Business](#)

# Plan for call admission control in Skype for Business Server

5/20/2019 • 16 minutes to read

Learn about call admission control, which can prevent calls from taking place if they would have poor media quality, in Skype for Business Server Enterprise Voice.

For IP-based applications such as telephony, video, and application sharing, the available bandwidth of enterprise networks is not generally considered to be a limiting factor within LAN environments. However, on WAN links that interconnect sites, network bandwidth can be limited.

When network traffic oversubscribes a WAN link, current mechanisms such as queuing, buffering, and packet dropping are used to resolve the congestion. The extra traffic is typically delayed until the network congestion eases or, if necessary, the traffic is dropped. For conventional data traffic in such situations, the receiving client can recover. However, for real-time traffic such as unified communications, network congestion cannot be resolved in this manner, because the unified communications traffic is sensitive to both latency and packet loss. Congestion on the WAN can result in a poor Quality of Experience (QoE) for users. For real-time traffic in congested conditions, it is actually better to deny calls than to provide connections with poor quality.

Call admission control (CAC) determines whether there is sufficient network bandwidth to establish a real-time session of acceptable quality. In Skype for Business Server, CAC controls real-time traffic only for audio and video, but it does not affect data traffic. If the default WAN path does not have the required bandwidth, CAC can attempt to route the call through an Internet path or the public switched telephone network (PSTN).

This section describes the call admission control functionality and explains how to plan for CAC.

## NOTE

Skype for Business Server has three advanced Enterprise Voice features: call admission control (CAC), emergency services (E9-1-1), and media bypass. For an overview of planning information that is common to all three of these features, see [Network settings for the advanced Enterprise Voice features in Skype for Business Server](#).

The CAC design in Skype for Business Server offers four main attributes:

- It is simple to deploy and manage without requiring additional equipment, such as specially configured routers.
- It addresses critical unified communications use cases, such as roaming users and multiple points of presence. CAC policies are enforced according to where the endpoint is located, not where the user is homed.
- In addition to voice calls, it can be applied to other traffic, such as video calls and audio/video conferencing sessions.
- Provides the flexibility to enable representation of various kinds of network topologies.

If a new voice or video session exceeds the bandwidth limits that you have set on a WAN link, the session is either blocked or (for phone calls only) rerouted to the PSTN.

CAC controls real-time traffic for voice and video only. It does not control data traffic.

Administrators define CAC policies, which are enforced by the Bandwidth Policy Service that is installed with

every Front End pool. CAC settings are automatically propagated to all Skype for Business Server Front End Servers in your network.

For calls that fail because of CAC policies, the order of precedence for rerouting the call is as follows:

1. Internet
2. PSTN
3. Voice mail

Call detail recording (CDR) captures information about calls that are rerouted to the PSTN or to voice mail. CDR does not capture information about calls that are rerouted to the Internet, because the Internet is treated as an alternate path rather than a secondary option.

#### NOTE

Voice mail deposits will not be denied because of bandwidth constraints.

The Bandwidth Policy Service generates two types of log files in comma separated values (CSV) format. The **check failures** log file captures information when bandwidth requests are denied. The **link utilization** log file captures a snapshot of the network topology and the WAN link bandwidth utilization. Both of these log files can assist you in fine-tuning your CAC policies based on utilization.

## Call Admission Control Considerations

The administrator selects to install the Bandwidth Policy Service on the first pool configured in the central site. Since there is a single central site per network region, there is only one Bandwidth Policy Service per network region, which manages bandwidth policy for that region, its associated sites and the links to those sites. The Bandwidth Policy Service runs as part of the Front End Servers, and therefore high availability is built-in within that pool. The Bandwidth Policy Service running on each Front End Server synchronizes every 15 seconds. If the Front End pool fails, CAC policies are no longer enforced for that site until the Front End pool and consequently the Bandwidth Policy Service becomes operational again. This implies that all calls will go through for the duration the Bandwidth Policy Service is out of service. Therefore there is the possibility of bandwidth oversubscription of your links during this period

The Bandwidth Policy Service provides high availability within a Front End pool; however, it does not provide redundancy across Front End pools. The Bandwidth Policy Service cannot failover from one Front End pool to another. Once service to the Front End pool is restored, the Bandwidth Policy Service is resumed and can enforce bandwidth policy checks again.

### Network Considerations

Although bandwidth restriction for audio and video is enforced by the Bandwidth Policy Service in Skype for Business Server, this restriction is not enforced at the network router (layer 2 and 3). CAC cannot prevent a data application, for example, from consuming the entire network bandwidth on a WAN link, including the bandwidth that is reserved for audio and video by your CAC policy. To protect the necessary bandwidth on your network, you can deploy a Quality of Service (QoS) protocol such as Differentiated Services (DiffServ). Therefore, a best practice is to coordinate the CAC bandwidth policies you define with any QoS settings that you might deploy.

### Media and Signaling Paths over VPN

If your enterprise supports media through VPN, ensure that either both the media stream and the signaling stream go through the VPN or both are routed through the internet. By default, the media and signaling streams go through the VPN tunnel.

### Call Admission Control of Outside Users

Call admission control is not enforced beyond the limits of the Skype for Business Server organization. CAC cannot be applied to the media traffic traversing the Internet, which is not managed by Skype for Business Server. CAC checks will be performed on the portion of the call that flows through the enterprise network if the called endpoint belongs to the organization, and the Edge Server has been added to the network configuration, as described in [Call admission control deployment: final checklist for Skype for Business Server](#). If the called endpoint doesn't belong to the organization, such as a federated or PIC user, no bandwidth policy checks are performed and the outgoing call will ignore any CAC restrictions.

### Call Admission Control of PSTN Connections

Call admission control is enforceable on the Mediation Server regardless of whether it is connected to an IP/PBX, a PSTN gateway, or a SIP trunk. Because the Mediation Server is a back-to-back user agent (B2BUA), it terminates media. It has two connection sides: a side that is connected to Skype for Business Server and a gateway side, which is connected to PSTN gateways, IP/PBXs, or SIP trunks. For details about PSTN connections, see [Plan for PSTN connectivity in Skype for Business Server](#).

CAC can be enforced on both sides of the Mediation Server unless media bypass is enabled. If media bypass is enabled, the media traffic doesn't traverse the Mediation Server but instead flows directly between the Skype for Business client and the gateway. In this case, CAC is not needed. For details, see [Plan for media bypass in Skype for Business](#).

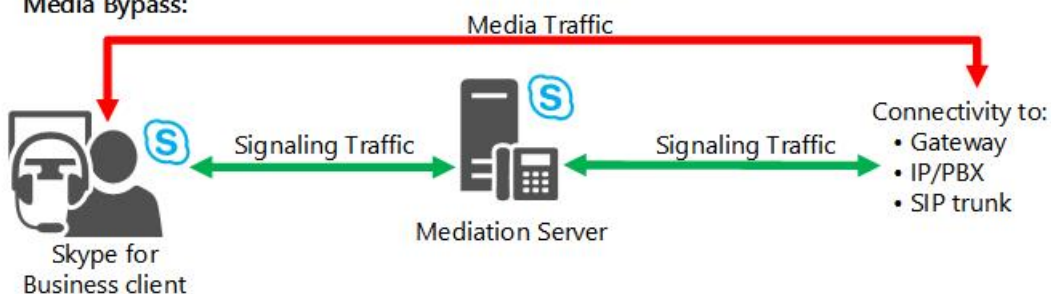
The following figure illustrates how CAC is enforced on PSTN connections with and without media bypass enabled.

### Call admission control enforcement on connections to the PSTN

#### No Media Bypass:



#### Media Bypass:



## Defining your requirements for call admission control

Planning for call admission control (CAC) requires detailed information about your enterprise network topology. To help plan your call admission control policies, follow these steps.

1. Identify the hubs/backbones (called network regions) within your enterprise network.
2. Identify the offices or locations (called network sites) within each network region.
3. Determine the network route between every pair of network regions.
4. Determine the bandwidth limits for each WAN link.

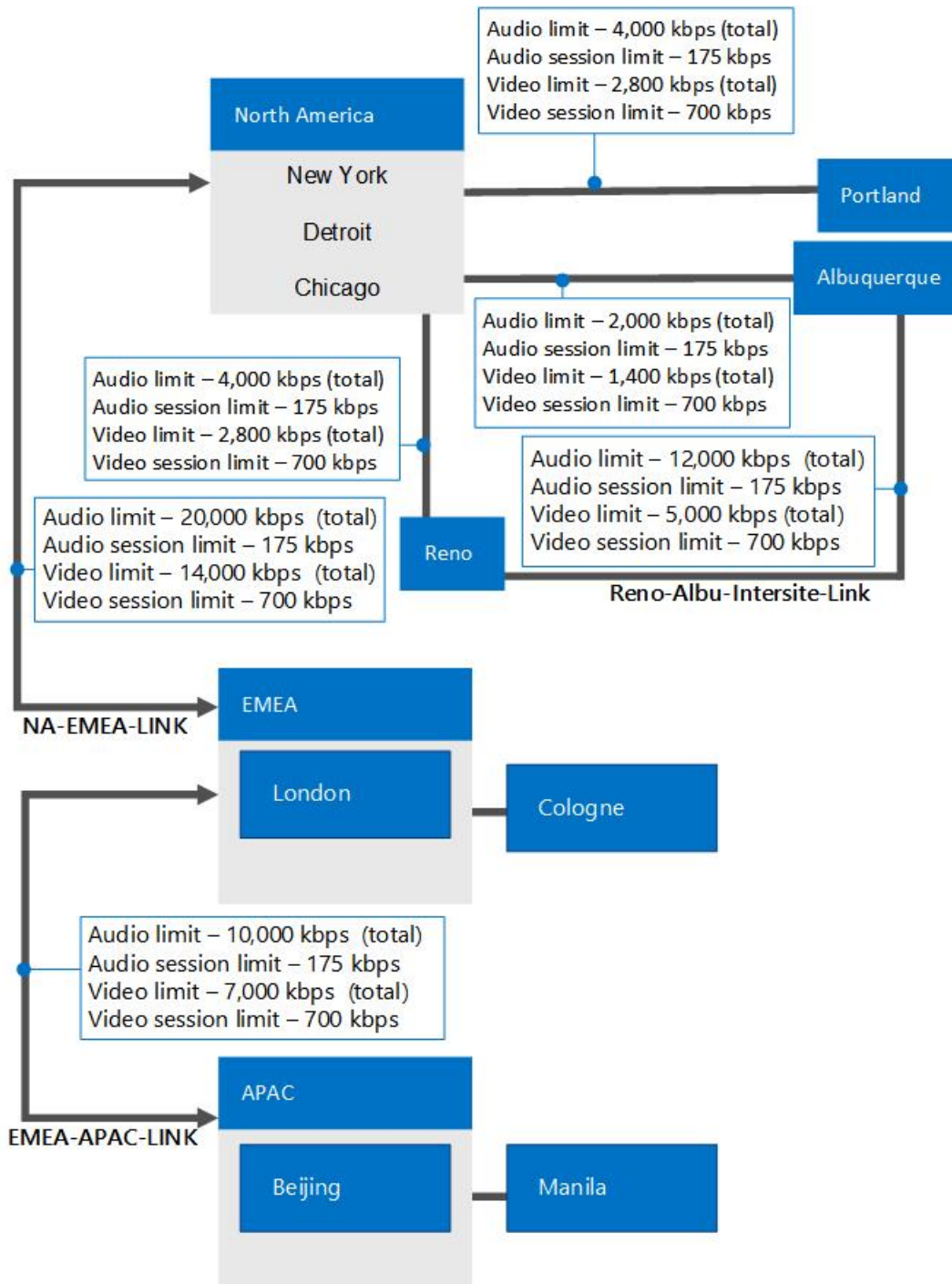
**NOTE**

Bandwidth limits refer to how much of the bandwidth on a WAN link is allocated to Enterprise Voice and audio/video traffic. When a WAN link is described as "bandwidth-constrained," the WAN link has a bandwidth limit that is lower than the expected peak traffic over the link.

5. Identify the IP subnets that are assigned to each network site.

To explain these concepts, we'll use the example network topology shown in the following figure.

**Example topology for call admission control**



**NOTE**

All network sites are associated with a network region. For example, Portland, Reno, and Albuquerque are included in the North America region. In this figure, only WAN links that have CAC policies applied are shown, with bandwidth limits. The network sites of Chicago, New York, and Detroit are shown inside the North America region oval because they are not bandwidth-constrained, and therefore do not require CAC policies.

The components of this example topology are explained in the following sections. For details about how this topology was planned, including the bandwidth limits, see [Example: Gathering requirements for call admission control in Skype for Business Server](#).

**Identify Network Regions**

A network region represents a network backbone or a network hub.

A network backbone or hub is a part of computer network infrastructure that interconnects different parts of the network, providing a path for the exchange of information between different LANs or subnets. A backbone can tie together diverse networks from a small location to a wide geographic area. The backbone's capacity is typically greater than that of the networks that connect to it.

Our example topology has three network regions: North America, EMEA, and APAC. A network region contains a collection of network sites (see the definition of network sites later in this topic). Work with your network operations team to identify your network regions.

**Associating a Central Site with each Network Region**

CAC requires that a Skype for Business Server central site is defined for each network region. The central site is selected with the best network connectivity and highest bandwidth to all the other sites within that network region. The preceding example of network topology shows three network regions, each with a central site that manages CAC decisions. From the preceding example, the appropriate association is shown in the following table.

**NOTE**

Central sites do not necessarily correspond to network sites. In the examples in this documentation, some central sites—Chicago, London, and Beijing—share the same name as the network sites. However, even if a central site and network site share the same name, the central site is an element of the Skype for Business Server topology, whereas the network site is a part of the overall network in which the Skype for Business Server topology resides.

**Network regions, central sites, and network sites**

NETWORK REGION	CENTRAL SITE	NETWORK SITES
North America	Chicago	Chicago New York Detroit Portland Reno Albuquerque
EMEA	London	London Cologne
APAC	Beijing	Beijing Manila

**Identify Network Sites**



A network site represents a location where your organization has a physical venue—for example, offices, a set of buildings, or a campus. A physical venue with a LAN and has WAN connectivity to other sites is considered a network site. Start by inventorying all of your organization's offices. In our example topology, the North America network region consists of the following network sites: New York, Chicago, Detroit, Portland, Reno, and Albuquerque.

You must associate every network site with a network region. Depending on whether the network site has a constrained WAN link, a bandwidth policy is associated with the network site. For details about CAC policies and the bandwidth that you allocate by using them, see "Define Bandwidth Policies" later in this topic. To configure CAC, you associate network sites with network regions, and then you create bandwidth-allocating policies to apply to the bandwidth-constrained connections between a given site or region and the WAN connections between the sites and regions.

### Identify Network Links

Network links represent connections to the physical WAN that links different regions and sites. In our example topology, there are two regional network links, five network links between regions and sites, and one network link between two sites.

The two regional links are between North America and EMEA, represented as NA-EMEA-LINK, and between APAC and EMEA, represented as EMEA-APAC-LINK.

The site links are indicated by the lines connecting Portland, Reno, and Albuquerque to the North America region, Manila to the APAC region, and Cologne to the EMEA region. The line between Reno and Albuquerque shows a direct network link between these two sites.

### Define Bandwidth Policies

Work with your network operations team to determine how much WAN bandwidth is available for real-time audio and video traffic across the WAN links in your organization. Bandwidth policies are typically applied to WAN links if the bandwidth usage is constrained; that is, if it is expected to be more than the bandwidth that can be allocated for audio and video modalities.

CAC bandwidth policies define the maximum bandwidth that can be reserved for real-time audio and video modalities. Since CAC does not limit the bandwidth of other traffic, it cannot prevent other data traffic such as a large file transfer, music streaming, from using up all of the network bandwidth.

CAC bandwidth policies can define any or all of the following:

- Maximum total bandwidth allocated for audio.
- Maximum total bandwidth allocated for video.
- Maximum bandwidth allocated for a single audio call (session).
- Maximum bandwidth allocated for a single video call (session).

#### NOTE

All CAC bandwidth values represent the maximum *unidirectional* bandwidth limits.

## NOTE

The Skype for Business Server Voice Policy features provide the ability to override bandwidth policy checks for incoming calls to the user (not for outgoing calls that are placed by the user). After the session is established, the bandwidth consumption will be accurately accounted for. This setting should be used sparingly. For details, see [Create or modify a voice policy and configure PSTN usage records in Skype for Business](#) or [Modify a Voice Policy and Configure PSTN Usage Records](#) in the Deployment documentation.

To optimize bandwidth utilization on a per-session basis, consider the type of audio and video codecs that will be used. In particular, avoid allocating insufficient bandwidth for a codec that you expect to be used frequently. Conversely, if you want to prevent media from using a codec that requires more bandwidth, you should set the maximum bandwidth per session low enough to discourage such use. For audio, not every codec is available for every scenario. For example:

- Peer-to-peer audio calls between Skype for Business endpoints will use either RTAudio (8kHz) or RTAudio (16kHz) when you factor in the bandwidth and prioritization of codecs.
- Conference calls between Skype for Business endpoints and the A/V Conferencing service will use either G.722 or Siren.
- Calls to the public switched telephone network (PSTN) either to or from Skype for Business endpoints will use either G.711 or RTAudio (8kHz).

Use the following table to help optimize the maximum per-session bandwidth settings.

### Bandwidth utilization by codecs

CODEC	BANDWIDTH REQUIREMENT WITH NO FORWARD ERROR CORRECTION (FEC)	BANDWIDTH REQUIREMENT WITH FORWARD ERROR CORRECTION (FEC)
RTAudio (8kHz)	49.8 kbps	61.6 kbps
RTAudio (16kHz)	67 kbps	96 kbps
Siren	57.6 kbps	73.6 kbps
G.711	102 kbps	166 kbps
G.722	105.6 kbps	169.6 kbps
RTVideo (CIF 15 fps)	260 kbps	Not applicable
RTVideo (VGA 30 fps)	610 kbps	Not applicable

## NOTE

Bandwidth requirements take into account overhead for the following: Ethernet II, IP, User Datagram Protocol (UDP), RTP (real-time transport protocol), and SRTP (secure real-time transport protocol). They also include 10 kbps for RTCP overhead.

The G.722.1 and Siren codecs are similar, but they offer different bit rates.

G.722, the default codec for Skype for Business Server conferencing, is completely different from the G.722.1 and Siren codecs.

The Siren codec is used in Skype for Business Server in the following situations:

- If the bandwidth policy is set too low for G.722 to be used.
- If a Communications Server 2007 or Communications Server 2007 R2 client connects to a Skype for Business Server conferencing service (because those clients do not support the G.722 codec).

### Bandwidth utilization by scenario

SCENARIO	BANDWIDTH REQUIREMENT OPTIMIZED FOR QUANTITY (KBPS)	BANDWIDTH REQUIREMENT FOR BALANCED MODE (KBPS)	BANDWIDTH REQUIREMENT OPTIMIZED FOR QUALITY (KBPS)
Peer-to-peer audio calls	45 kbps	62 kbps	91 kbps
Conference calls	53 kbps	101 kbps	165 kbps
PSTN calls (between Skype for Business and PSTN gateway, with media bypass)	97 kbps	97 kbps	161 kbps
PSTN calls (between Skype for Business and Mediation Server, without media bypass)	45 kbps	97 kbps	161 kbps
PSTN calls (between Mediation Server and PSTN gateway, without media bypass)	97 kbps	97 kbps	161 kbps
Skype for Business - Polycom calls	101 Kbps	101 Kbps	101 Kbps

### Identify IP Subnets

For each network site, you will need to work with your network administrator to determine what IP subnets are assigned to each network site. If your network administrator has already organized the IP subnets into network regions and network sites, then your work is significantly simplified.

In our example, the New York site in the North America region is assigned the following IP subnets: 172.29.80.0/23, 157.57.216.0/25, 172.29.91.0/23, 172.29.81.0/24. Suppose Bob, who typically works in Detroit, travels to the New York office for training. When he turns on his computer and connects to the network, his computer will get an IP address in one of the four ranges reserved for New York, for example 172.29.80.103.

#### Caution

The IP subnets specified during network configuration on the server must match the format provided by client computers in order to be properly used for media bypass. A Skype for Business client takes its local IP address and masks the IP address with the associated subnet mask. When determining the bypass ID associated with each client, the Registrar will compare the list of IP subnets associated with each network site against the subnet provided by the client for an exact match. For this reason, it is important that subnets entered during network configuration on the server are actual subnets instead of virtual subnets. (If you deploy call admission control, but not media bypass, call admission control will function properly even if you configure virtual subnets.) For example, if a client signs in on a computer with an IP address of 172.29.81.57 with an IP subnet mask of 255.255.255.0, Skype for Business will request the bypass ID associated with subnet 172.29.81.0. If the subnet is defined as 172.29.0.0/16, although the client belongs to the virtual subnet, the Registrar will not consider this a match because the Registrar is specifically looking for subnet 172.29.81.0. Therefore, it is important that the

administrator enters subnets exactly as provided by Skype for Business clients (which are provisioned with subnets during network configuration either statically or by DHCP.)

## Best practices for call admission control

To enhance performance and facilitate deployment, apply the following best practices when you deploy call admission control:

- Ensure that WANs are adequately provisioned for current and anticipated media traffic.

### NOTE

We recommend that you factor in a buffer to your bandwidth limits. There are scenarios such as race conditions that affect the total bandwidth used and can result in situations where the bandwidth limit is exceeded. For example, if two calls try to start while media traffic is approaching a bandwidth limit, one of them may be denied because the other managed to start first.

- Monitor network usage and call detail records so that you can choose optimal CAC settings and update CAC settings as network usage changes.
- Use CAC bandwidth policies to complement QoS settings.
- If you want to re-route blocked calls onto the PSTN, verify PSTN functionality and capacity. For details, see [Planning Outbound Call Routing](#).

### NOTE

Capacity refers to the number of ports you need to open to support potential PSTN re-routing.

# Example: Gathering requirements for call admission control in Skype for Business Server

5/20/2019 • 10 minutes to read

Provides a detailed example of planning for call admission control in Skype for Business Server Enterprise Voice, including gathering information about your network's sites, regions, and bandwidth.

This example shows you how to plan for and implement call admission control (CAC). At a high level, this consists of the following activities:

1. Identify all of your network hubs and backbones (known as network regions).
2. Identify the Skype for Business Server central site that will manage CAC for each network region.
3. Identify and define the network sites that are connected to each network region.
4. For each network site whose connection to the WAN is bandwidth-constrained, describe the bandwidth capacity of the WAN connection and the bandwidth limits that the network administrator has set for Skype for Business Server media traffic, if applicable. You do not need to include sites whose connection to the WAN is not bandwidth-constrained.
5. Associate each subnet in your network with a network site.
6. Map the links between the network regions. For each link, describe its bandwidth capacity and any limits that the network administrator has placed on Skype for Business Server media traffic.
7. Define a route between every pair of network regions.

## Gather the Required Information

To prepare for call admission control, gather the information described in the following steps:

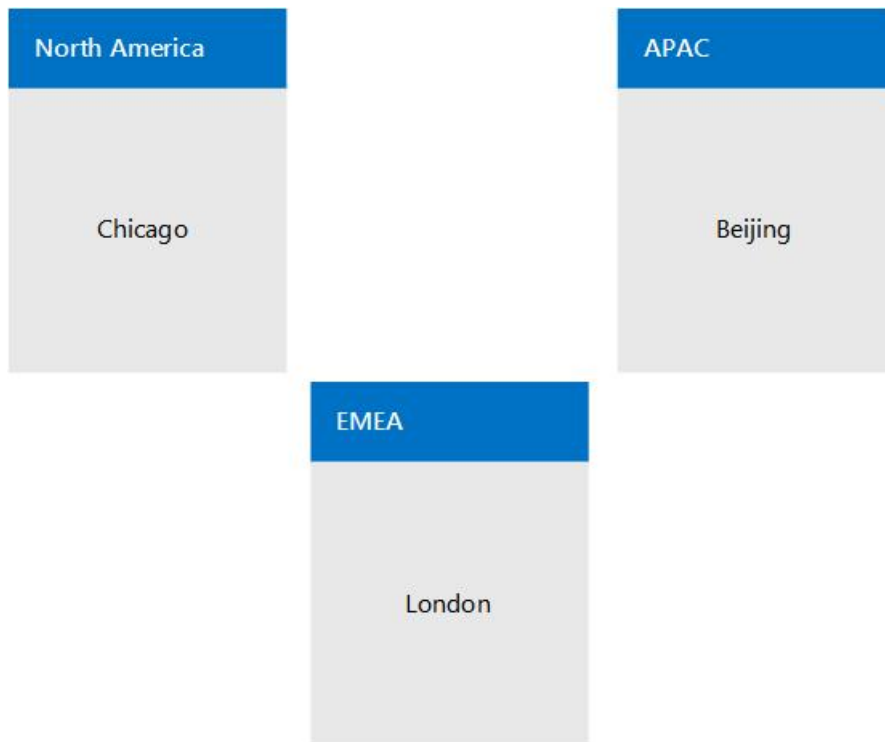
1. Identify your network regions. A network region represents a network backbone or a network hub.

A network backbone or a network hub is a part of computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnets. A backbone can tie together diverse networks, from a small location to a wide geographic area. The backbone's capacity is typically greater than that of the networks connected to it.

Our example topology has three network regions: North America, EMEA, and APAC. A network region contains a collection of network sites. Work with your network administrator to define the network regions for your enterprise.

2. Identify each network region's associated central site. A central site contains at least one Front End Server and is the Skype for Business Server deployment that will manage CAC for all media traffic that passes through the network region's WAN connection.

**An example enterprise network divided into three network regions**



**NOTE**

A Multiprotocol Label Switching (MPLS) network should be represented as a network region in which each geographic location has a corresponding network site. For details, see [Components and topologies for call admission control in Skype for Business](#).

In the preceding example network topology, there are three network regions, each with a Skype for Business Server central site that manages CAC. The appropriate central site for a network region is chosen by the geographic vicinity. Because media traffic will be heaviest within network regions, the ownership by geographic vicinity makes it self-contained and will continue to be functional even if other central sites become unavailable.

In this example, a Skype for Business deployment named Chicago is the central site for the North America region.

All Skype for Business users in North America are homed on servers in the Chicago deployment. The following table shows central sites for all three network regions.

**Network Regions and their Associated Central Sites**

NETWORK REGION	CENTRAL SITE
North America	Chicago
EMEA	London
APAC	Beijing

**NOTE**

Depending on your Skype for Business Server topology, the same central site can be assigned to multiple network regions.

- For each network region, identify all of the network sites (offices or locations) whose WAN connections are not bandwidth-constrained. Because these sites are not bandwidth constrained, you do not need to apply CAC bandwidth policies to them.

In the example shown in the following table, three network sites do not have bandwidth-constrained WAN links: New York, Chicago, and Detroit.

**Network Sites not Constrained by WAN Bandwidth**

NETWORK SITE	NETWORK REGION
New York	North America
Chicago	North America
Detroit	North America

- For each network region, identify all of the network sites that connect to the network region through bandwidth-constrained WAN links.

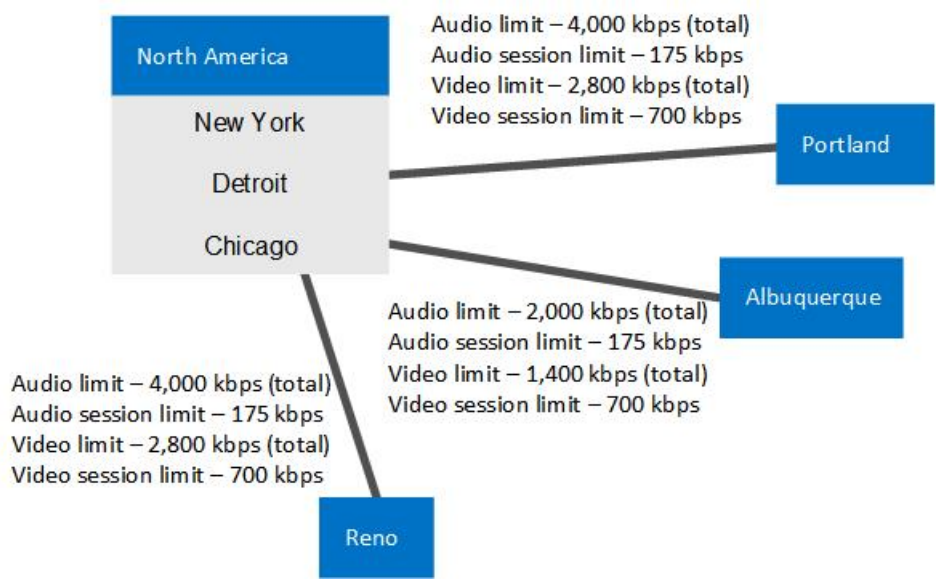
To help ensure audio and video quality, we recommend that these bandwidth-constrained network sites have their WANs monitored and CAC bandwidth policies that limit media (voice or video) traffic flow to and from the network region.

In the example shown in the following table, there are three network sites that are constrained by WAN bandwidth: Portland, Reno and Albuquerque.

**Network Sites Constrained by WAN Bandwidth**

NETWORK SITE	NETWORK REGION
Albuquerque	North America
Reno	North America
Portland	North America

**CAC network region North America with three network sites that are unconstrained by bandwidth (Chicago, New York, and Detroit) and three network sites that are constrained by WAN bandwidth (Portland, Reno, and Albuquerque)**



5. For each bandwidth-constrained WAN link, determine the following:

- Overall bandwidth limit that you want to set for all concurrent audio sessions. If a new audio session will cause this limit to be exceeded, Skype for Business Server does not allow the session to start.
- Bandwidth limit that you want to set for each individual audio session. The default CAC bandwidth limit is 175 kbps, but it can be modified by the administrator.
- Overall bandwidth limit that you want to set for all concurrent video sessions. If a new video session will cause this limit to be exceeded, Skype for Business Server does not allow the session to start.
- Bandwidth limit that you want to set for each individual video session. The default CAC bandwidth limit is 700 kbps, but it can be modified by the administrator.

**Network Sites with WAN Bandwidth Constraint Information (Bandwidth in kbps)**

NETWORK SITE	NETWORK REGION	BW LIMIT	AUDIO LIMIT	AUDIO SESSION LIMIT	VIDEO LIMIT	VIDEO SESSION LIMIT
Albuquerque	North America	5,000	2,000	175	1,400	700
Reno	North America	10,000	4,000	175	2,800	700
Portland	North America	5,000	4,000	175	2,800	700
New York	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)
Chicago	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)
Detroit	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)

6. For every subnet in your network, specify its associated network site.

**IMPORTANT**

Every subnet in your network must be associated with a network site, even if the network site is not bandwidth constrained. This is because call admission control uses subnet information to determine at which network site an endpoint is located. When the locations of both parties in the session are determined, call admission control can determine if there is sufficient bandwidth to establish a call. When a session is established over a link that has no bandwidth limits, an alert is generated.



**IMPORTANT**

If you deploy Audio/Video Edge Servers, the public IP addresses of each Edge Server must be associated with the network site where the Edge Server is deployed. Each public IP address of the A/V Edge Server must be added to your network configuration settings as a subnet with a subnet mask of 32. For example, if you deploy A/V Edge Servers in Chicago, then for each external IP address of those servers create a subnet with a subnet mask of 32 and associate network site Chicago with those subnets. For details about public IP addresses, see [Plan network requirements for Skype for Business](#).

A Key Health Indicator (KHI) alert is raised, specifying a list of IP addresses that are present in your network but are either not associated with a subnet, or the subnet that includes the IP addresses is not associated with a network site. This alert will not be raised more than once within an 8 hour period. The relevant alert information and an example are as follows:

**Source:** CS Bandwidth Policy Service (Core)

**Event number:** 36034

**Level:** 2

**Description:** The subnets for the following IP Addresses: <List of IP Addresses> are either not configured or the subnets are not associated to a network site.

**Cause:** The subnets for the corresponding IP addresses are missing from the network configuration settings or the subnets are not associated to a network site.

**Resolution:** Add subnets corresponding to the preceding list of IP addresses into the network configuration settings and associate every subnet to a network site.

For example, if the IP address list in the alert specifies 10.121.248.226 and 10.121.249.20, either these IP addresses are not associated with a subnet, or the subnet that they are associated with does not belong to a network site. If 10.121.248.0/24 and 10.121.249.0/24 are the corresponding subnets for these addresses, you can resolve this issue as follows:

- a. Be sure that IP address 10.121.248.226 is associated with the 10.121.248.0/24 subnet and IP address 10.121.249.20 is associated with the 10.121.249.0/24 subnet.
- b. Be sure that the 10.121.248.0/24 and 10.121.249.0/24 subnets are each associated with a network site.

**Network Sites and Associated Subnets (Bandwidth in kbps)**

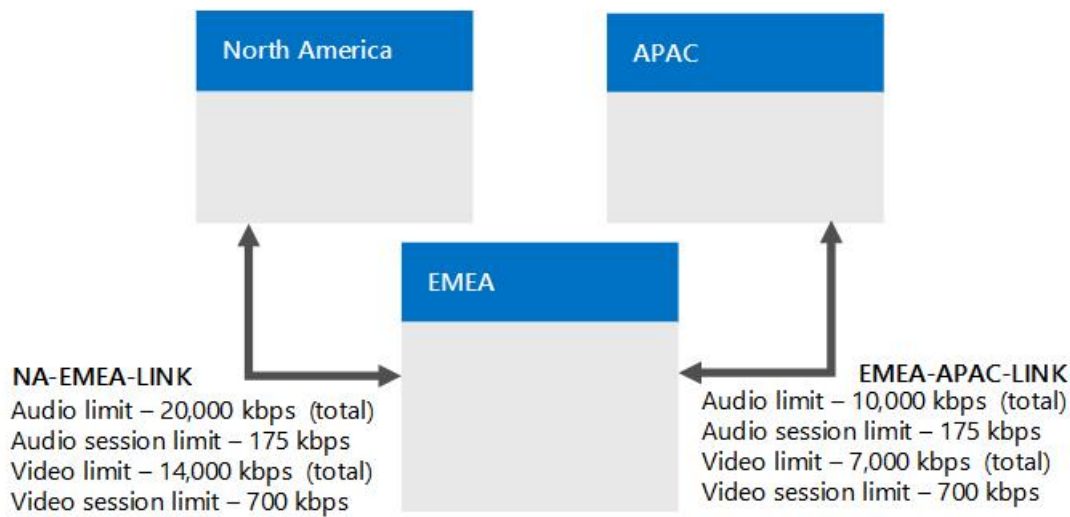
NETWORK SITE	NETWORK REGION	BW LIMIT	AUDIO LIMIT	AUDIO SESSION LIMIT	VIDEO LIMIT	VIDEO SESSION LIMIT	SUBNETS
Albuquerque	North America	5,000	2,000	175	1,400	700	172.29.79.0/23, 157.57.215.0/25, 172.29.90.0/23, 172.29.80.0/24
Reno	North America	10,000	4,000	175	2,800	700	157.57.210.0/23, 172.28.15.1.128/25

NETWORK SITE	NETWORK REGION	BW LIMIT	AUDIO LIMIT	AUDIO SESSION LIMIT	VIDEO LIMIT	VIDEO SESSION LIMIT	SUBNETS
Portland	North America	5,000	4,000	175	2,800	700	172.29.77.0/24 10.71.108.0/24, 157.57.208.0/23
New York	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)	172.29.80.0/23, 157.57.216.0/25, 172.29.91.0/23, 172.29.81.0/24
Chicago	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)	157.57.211.0/23, 172.28.152.128/25
Detroit	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)	172.29.78.0/24 10.71.109.0/24, 157.57.209.0/23

7. In Skype for Business Server call admission control, the connections between network regions are called region links. For each region link, determine the following, just as you did for the network sites:

- Overall bandwidth limit that you want to set for all concurrent audio sessions. If a new audio session will cause this limit to be exceeded, Skype for Business Server does not allow the session to start.
- Bandwidth limit that you want to set for each individual audio session. The default CAC bandwidth limit is 175 kbps, but it can be modified by the administrator.
- Overall bandwidth limit that you want to set for all concurrent video sessions. If a new video session will cause this limit to be exceeded, Skype for Business Server does not allow the session to start.
- Bandwidth limit that you want to set for each individual video session. The default CAC bandwidth limit is 700 kbps, but it can be modified by the administrator.

#### **Network Region links with associated bandwidth limits**



**Region Link Bandwidth Information (Bandwidth in kbps)**

REGION LINK NAME	FIRST REGION	SECOND REGION	BW LIMIT	AUDIO LIMIT	AUDIO SESSION LIMIT	VIDEO LIMIT	VIDEO SESSION LIMIT
NA-EMEA-LINK	North America	EMEA	50,000	20,000	175	14,000	700
EMEA-APAC-LINK	EMEA	APAC	25,000	10,000	175	7,000	700

8. Define a route between every pair of network regions.

**NOTE**

Two links are required for the route between the North America and APAC regions because there is no region link that directly connects them.

**Region Routes**

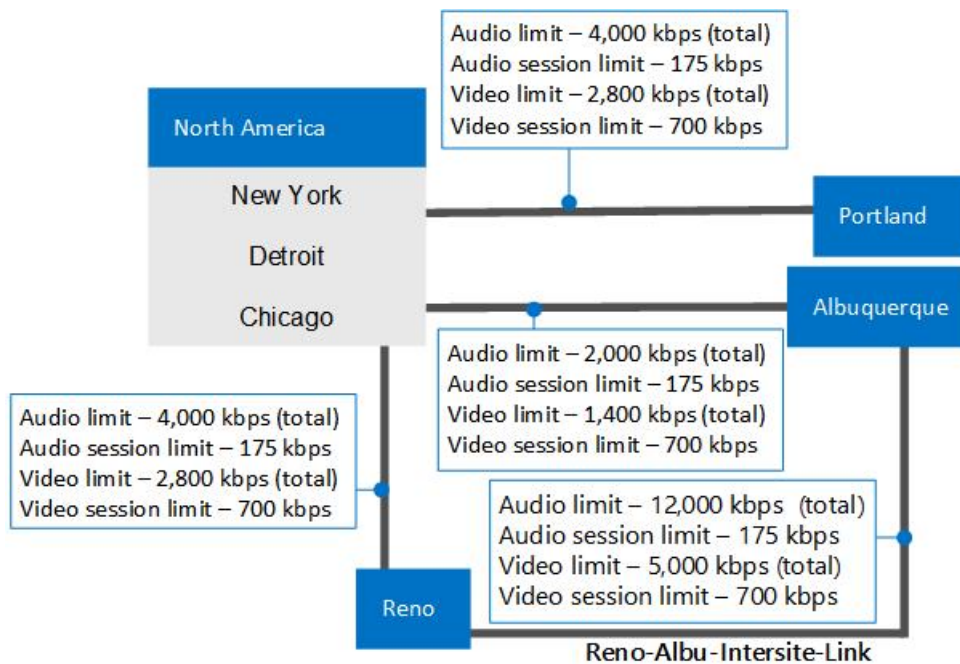
REGION ROUTE NAME	FIRST REGION	SECOND REGION	REGION LINKS
NA-EMEA-ROUTE	North America	EMEA	NA-EMEA-LINK
EMEA-APAC-ROUTE	EMEA	APAC	EMEA-APAC-LINK
NA-APAC-ROUTE	North America	APAC	NA-EMEA-LINK, EMEA-APAC-LINK

9. For every pair of network sites that are directly connected by a single link (called an inter-site link), determine the following:
- Overall bandwidth limit that you want to set for all concurrent audio sessions. If a new audio session will cause this limit to be exceeded, Skype for Business Server does not allow the session to start.
  - Bandwidth limit that you want to set for each individual audio session. The default CAC bandwidth limit is 175 kbps, but it can be modified by the administrator.
  - Overall bandwidth limit that you want to set for all concurrent video sessions. If a new video session

will cause this limit to be exceeded, Skype for Business Server does not allow the session to start.

- Bandwidth limit that you want to set for each individual video session. The default CAC bandwidth limit is 700 kbps, but it can be modified by the administrator.

**CAC network region North America showing the bandwidth capacities and bandwidth limits for the inter-site link between Reno and Albuquerque**



**Bandwidth Information for an Inter-Site Link between Two Network Sites (Bandwidth in kbps)**

INTER-SITE LINK NAME	FIRST SITE	SECOND SITE	BW LIMIT	AUDIO LIMIT	AUDIO SESSION LIMIT	VIDEO LIMIT	VIDEO SESSION LIMIT
Reno-Albu-Intersite-Link	Reno	Albuquerque	20,000	12,000	175	5,000	700

**Next Steps**

After you have gathered the required information, you can perform CAC deployment either by using the Skype for Business Server Management Shell or Skype for Business Server Control Panel.

**NOTE**

Although you can perform most network configuration tasks by using Skype for Business Server Control Panel, to create subnets and intersite links, you must use Skype for Business Server Management Shell. For details, see [New-CsNetworkSubnet](#) and [New-CsNetworkInterSitePolicy](#).

# Components and topologies for call admission control in Skype for Business

5/20/2019 • 6 minutes to read

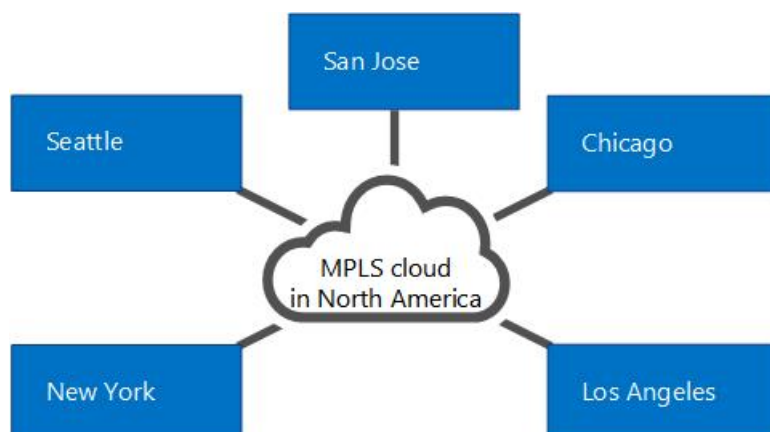
Planning for call admission control (CAC) if you have an MPLS network, a SIP trunk, or a third-party PSTN gateway or PBX. Applies to Skype for Business Server Enterprise Voice.

The topics in this section provide information about special considerations for deploying call admission control (CAC) with various types of network topologies.

## Call admission control on an MPLS network

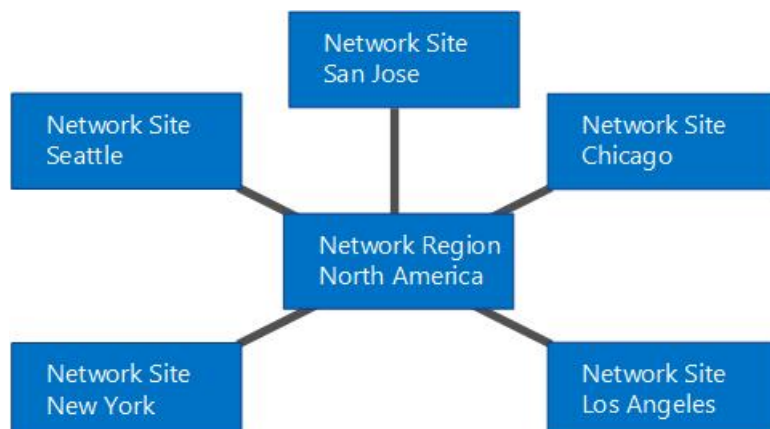
In a Multiprotocol Label Switching (MPLS) network, all sites are connected by a full-mesh. That is, all sites are connected directly to the MPLS backbone of the Internet service provider, and each site is provisioned bandwidth to be used across a WAN link to the MPLS cloud. There is no network hub or central site to control IP routing. The following figure shows a simple network based on MPLS technology.

### Example MPLS network



To deploy call admission control (CAC) in an MPLS network, you create a network region to represent the MPLS cloud, and create a network site to represent each MPLS satellite site. The following figure illustrates how the network region and network sites should be configured to represent the example MPLS network in the previous figure. The overall bandwidth limits and bandwidth session limits are then based on the capacity of the WAN link from each network site to the network region that represents the MPLS cloud.

### Network region and network sites for an MPLS network

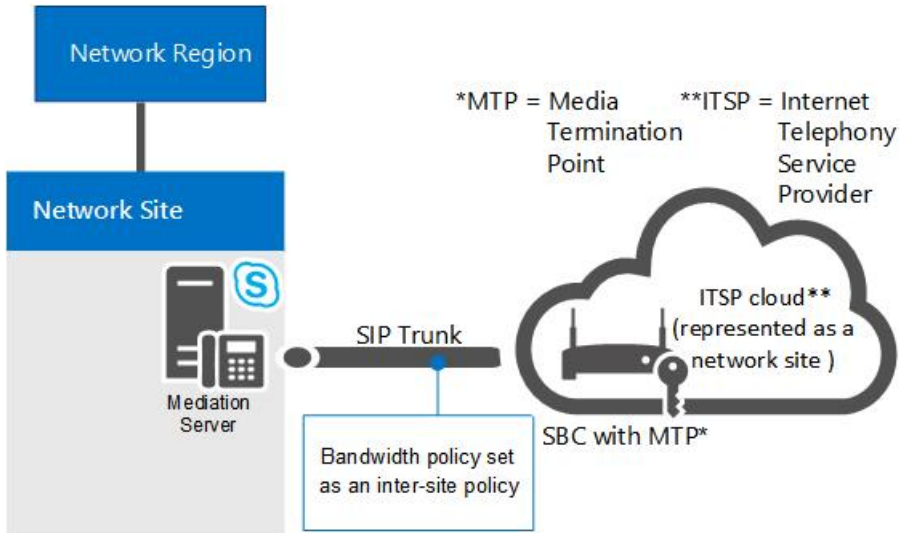


# Call admission control on a SIP trunk

To deploy call admission control (CAC) on a SIP trunk, you create a network site to represent the Internet telephony service provider (ITSP). To apply bandwidth policy values on the SIP trunk, you create an inter-site policy between the network site in your enterprise and the network site that you create to represent the ITSP.

The following figure shows an example CAC deployment on a SIP trunk.

## CAC configuration on a SIP trunk



To configure CAC on a SIP trunk, you will have to perform the following tasks during CAC deployment:

1. Create a network site to represent the ITSP. Associate the network site to an appropriate network region, and allocate bandwidth of zero for audio and video for this network site. For details, see [Configure Network Sites for CAC](#) in the Deployment documentation.

### NOTE

For the ITSP, this network site configuration is not functional. Bandwidth policy values are actually applied in step 2.

2. Create an inter-site link for the SIP trunk using the relevant parameter values for the site you created in step 1. For example, use the name of the network site in your enterprise as the value of the NetworkSiteID1 parameter, and the ITSP network site as the value of the NetworkSiteID2 parameter. For details, see [Create network intersite policies in Skype for Business Server](#) in the Deployment documentation, and [New-CsNetworkInterSitePolicy](#).
3. Get the IP address of the Session Border Controller's (SCB) Media Termination Point from your ITSP. Add that IP address with a subnet mask of 32 to the network site that represents the ITSP. For details, see [Associate a Subnet with a Network Site](#).

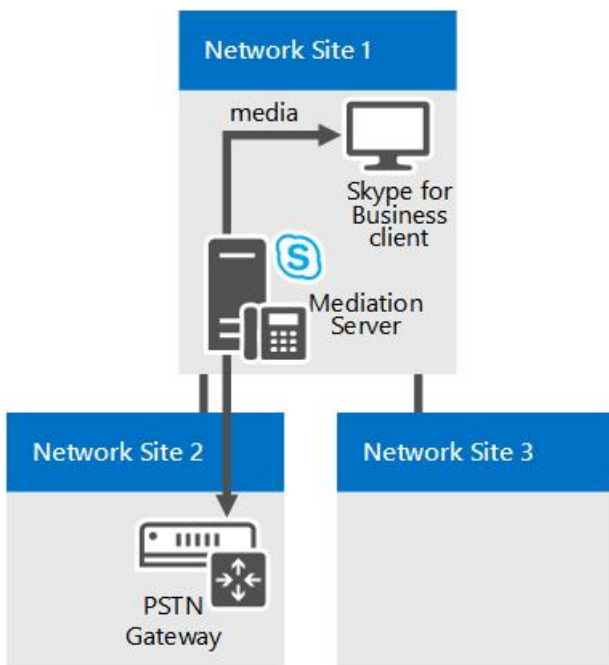
# Call admission control with a third-party PSTN gateway or PBX

This topic describes examples of how call admission control (CAC) can be deployed on the link between the Mediation Server's gateway interface and a third-party public switched telephone network (PSTN) gateway or private branch exchange (PBX).

## Case 1: CAC between the Mediation Server and a PSTN gateway

CAC can be deployed on the WAN link from the Mediation Server's gateway interface to a third-party PBX or PSTN gateway.

## Case 1: CAC between the Mediation Server and a PSTN gateway



In this example, CAC is applied between the Mediation Server and a PSTN gateway. If a Skype for Business client user at Network Site 1 places a PSTN call through the PSTN gateway in Network Site 2, the media flows through the WAN link. Therefore, two CAC checks are performed for each PSTN session:

- Between the Skype for Business client application and the Mediation Server
- Between the Mediation Server and the PSTN gateway

This works for both incoming PSTN calls to a client in Network Site 1, and for outgoing PSTN calls originating from a client application in Network Site 1.

#### NOTE

Make sure that the IP subnet that the PSTN gateway belongs to is configured and associated with Network Site 2.

#### NOTE

Make sure that the IP subnet that both interfaces of the Mediation Server belong to is configured and associated with Network Site 1.

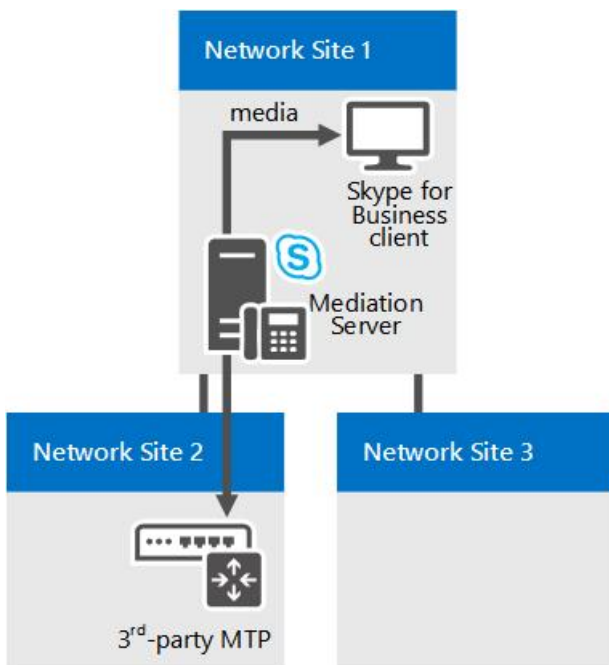
#### NOTE

For details, see [Associate a Subnet with a Network Site](#).

### Case 2: CAC between the Mediation Server and a third-party PBX with Media Termination Point

This configuration is similar to Case 1. In both the cases, the Mediation Server knows what device terminates media at the opposite end of the WAN link, and the IP address of the PSTN gateway or PBX with Media Termination Point (MTP) is configured on the Mediation Server as the next hop.

### Case 2: CAC between the Mediation Server and a third-party PBX with MTP



In this example, CAC is applied between the Mediation Server and the PBX/MTP. If a Skype for Business client user at the Network Site 1 places a PSTN call through the PBX/MTP located in Network Site 2, the media flows through the WAN link. Therefore, for each PSTN session two CAC checks are performed:

- Between the Skype for Business client application and the Mediation Server
- Between the Mediation Server and the PBX/MTP

This works for both incoming PSTN calls to a client in Network Site 1, and outgoing PSTN calls originating from a client in Network Site 1.

#### NOTE

Make sure that the IP subnet that the MTP belongs to is configured and associated with Network Site 2.

#### NOTE

Make sure that the IP subnet that both interfaces of the Mediation Server belong to is configured and associated with Network Site 1.

#### NOTE

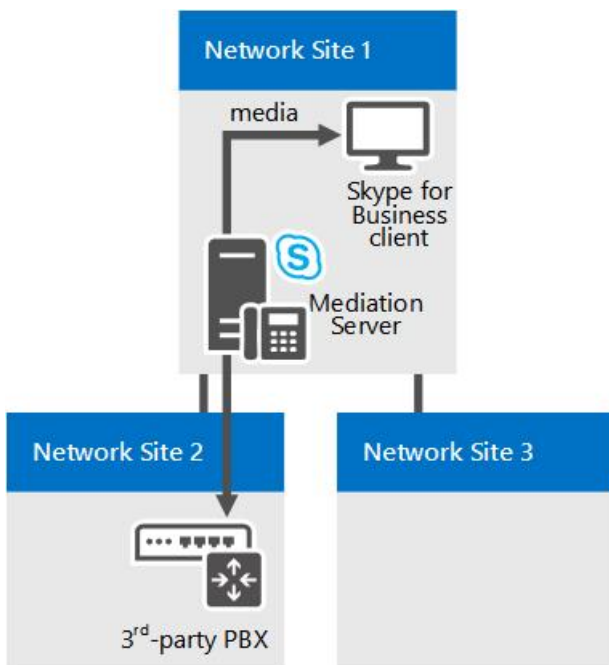
For details, see [Associate a Subnet with a Network Site](#).

### Case 3: CAC between the Mediation Server and a third-party PBX without a Media Termination Point

Case 3 is slightly different from the first two cases. If there is no MTP on the third-party PBX, for an outgoing session request to the third-party PBX the Mediation Server does not know where media will terminate in the PBX boundary. In this case, the media flows directly between the Mediation Server and the third-party endpoint device.

### Case 3: CAC between the Mediation Server and a third-party PBX without MTP





In this example, if a Skype for Business client user at Network Site 1 places a call to a user through the PBX, the Mediation Server is able to perform CAC checks only on the proxy leg (between the Skype for Business client application and Mediation Server). Because the Mediation Server does not have information about the endpoint device while the session is being requested, CAC checks cannot be performed on the WAN link (between the Mediation Server and the third-party endpoint) prior to call establishment. After the session is established, however, the Mediation Server facilitates in accounting for the bandwidth used on the trunk.

For calls that originate from the third-party endpoint, the information about that endpoint device is available at the time of session request and CAC check can be performed on both the sides of the Mediation Server.

**NOTE**

Make sure that the IP subnet that the endpoint devices belong to is configured and associated with Network Site 2.

**NOTE**

Make sure that the IP subnet that both interfaces of the Mediation Server belong to is configured and associated with Network Site 1.

**NOTE**

For details, see [Associate a Subnet with a Network Site](#).

# Plan for emergency services in Skype for Business Server

5/20/2019 • 12 minutes to read

Learn about Enhanced 9-1-1 (E9-1-1) services in Skype for Business Server Enterprise Voice, including location acquiring and call routing.

Skype for Business Server supports Enhanced 9-1-1 (E9-1-1) services within the United States as part of an Enterprise Voice deployment. E9-1-1 is an emergency dispatch feature that associates a 9-1-1 call with an Emergency Response Location (ERL) that consists of civic (that is, street) addresses and other more specific location information, such as floor numbers, for calls from office buildings and other multitenant facilities. By using the provided ERL, a Public Safety Answering Point (PSAP) can immediately dispatch first responders to the caller in distress with reduced risk of inadvertently directing the responder to an incorrect or ambiguous location.

## NOTE

Skype for Business Server now supports the configuration of multiple emergency numbers for a client. For more information see [Plan for multiple emergency numbers in Skype for Business Server](#).

## NOTE

Skype for Business Server has three advanced Enterprise Voice features: call admission control, emergency services (E9-1-1), and media bypass. For an overview of planning information that is common to all three of these features, see [Network settings for the advanced Enterprise Voice features in Skype for Business Server](#).

Skype for Business Server supports Enhanced 9-1-1 (E9-1-1) calling from Skype for Business clients and Lync Phone Edition devices. When you configure Skype for Business Server for E9-1-1, emergency calls placed from Skype for Business or Lync Phone Edition include Emergency Response Location (ERL) information from the Location Information service database. ERLs consist of civic (that is, street) addresses and other information that helps to identify a more precise location in office buildings and other multitenant facilities. When a user makes an emergency call, Skype for Business Server routes the call audio, along with the location and callback information, through a Mediation Server to an E9-1-1 service provider. The E9-1-1 service provider uses the civic address of the caller to route the call to the Public Safety Answering Point (PSAP) that serves the caller's location, and sends along an Emergency Service Query Key (ESQK) that the PSAP uses to look up the caller's ERL.

Skype for Business Server supports two methods for routing emergency calls to an E9-1-1 service provider:

- A Session Initiation Protocol (SIP) trunk connection to a qualified E9-1-1 service provider
- An Emergency Location Identification Number (ELIN) gateway to a public switched telephone (PSTN)-based E9-1-1 service provider

When you use a SIP trunk E9-1-1 service provider, you add ERLs to the Location Information service database, and then validate the locations against a Master Street Address Guide (MSAG) that is maintained by the E9-1-1 service provider. If an E9-1-1 service provider receives a call that doesn't have location information or has a location that has not been validated against the MSAG, the E9-1-1 service provider routes the call to a national/regional Emergency Call Response Center (ECRC), which is staffed with specially trained personnel who verbally obtain the caller's location, if possible, and manually route the call to the appropriate PSAP. (Some SIP trunk E9-1-1 service providers also provide customers with a PSTN direct inward dialing (DID) number to the

ECRC, which provides an alternate means of routing 9-1-1 calls, if the SIP trunk fails for any reason.)

Unlike time division multiplexing (TDM) and IP-based private branch exchange (PBX) phones, which have fixed locations, a Skype for Business endpoint can be very mobile. When you deploy the E9-1-1 feature, Skype for Business Server helps to ensure that no matter where a caller is located, the emergency call can be routed to the PSAP that serves the caller's location. For example, if a user's main office is located in Redmond, Washington, but the user places an emergency call from a computer in a branch office in Wichita, Kansas, the SIP trunk or PSTN-based E9-1-1 service provider will route the call to the PSAP in Wichita, not to the PSAP in Redmond.

When you use an ELIN gateway, you also add ERLs to the Location Information service database, but you include also an ELIN number for each location. The ELIN number becomes the emergency calling number during the emergency call. You must then make sure that your PSTN carrier uploads the ELINs to the Automatic Location Identification (ALI) database.

#### NOTE

Skype for Business-connected analog devices cannot receive location information from the Location Information service or transmit location to the E9-1-1 service provider.

If you use the SIP trunk E9-1-1 service provider option and need to support E9-1-1 from analog phones, you have two options:

- **Traditional PS-ALI option** If you have local PSTN gateways at each site where analog phones are deployed and each analog phone has a DID, you can provision the analog device's location directly with a Private Switch/Automatic Location Identification (PS-ALI) service provider. In this case, you configure specially-crafted Skype for Business voice policies and assign them to the analog device contact objects so that E9-1-1 calls from those phones route directly through the local gateway to the PSTN provider that services the site (instead of routing the call to an E9-1-1 service provider SIP trunk). When an emergency call is placed, a database at a PS-ALI provider that is associated with the PSTN trunk maps the DID of each analog phone to a physical location and provides this location to the PSAP. These records must be updated with the PS-ALI service provider every time phones are moved to different ERLs.
- **E9-1-1 service provider option** You can register the analog phone DIDs and their corresponding ERLs with the E9-1-1 service provider, if this is supported by the E9-1-1 service provider. If the provider receives a call from Skype for Business Server that doesn't include PIDF-LO data, the provider can see if there is a database match on the calling party's DID number. By using the ERL retrieved from its database, the provider can automatically route the emergency call to the correct PSAP, and the PSAP will receive the DID of the analog device and an ESQK record that allows the dispatcher to lookup the caller's location.

If you use the ELIN gateway option and need to support E9-1-1 from analog phones, you can provision the analog device's location directly with the PS-ALI service provider, as described in the first option above.

From a Skype for Business Server perspective, the E9-1-1 process can be separated into two stages:

- Stage 1: Acquiring a location
- Stage 2: Routing the emergency call to an E9-1-1 service provider

This section describes how these stages work.

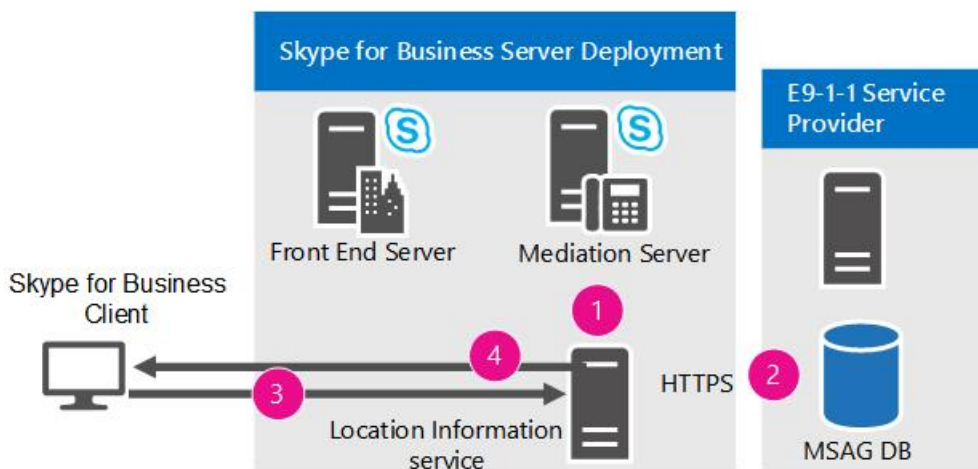
If you plan to configure your infrastructure to automatically detect client location, first you need to decide which network elements you will use to map callers to locations. For details about the possible options, see [Define the network elements used to determine location in Skype for Business Server](#).

## Acquiring a location

In a Skype for Business Server E9-1-1 deployment, each internally-connected Skype for Business or Lync Phone Edition client actively acquires its own location. After SIP registration, the client furnishes all the network connectivity information that it knows about itself in a location request to the Location Information service, which is a web service backed by a replicated SQL Server database. Each central site pool has a Location Information service, which uses the network information to query its records for a matching location. If there is a match, the Location Information service returns a location to the client. If there is not a match, the user may be prompted to enter a location manually (depending on location policy settings). The location data are transmitted back to the client in an Internet Engineering Task Force (IETF) standardized XML format called Presence Information Data Format Location Object (PIDF-LO).

The Skype for Business client includes the PIDF-LO data as part of an emergency call, and this data is used by the E9-1-1 service provider to determine the appropriate PSAP and route the call to that PSAP along with the correct ESQK, which allows the PSAP dispatcher to obtain the caller's location.

The following diagram shows how a Skype for Business client acquires a location (except for the third-party client MAC address-based location method):



For a client to acquire a location, the following steps must take place:

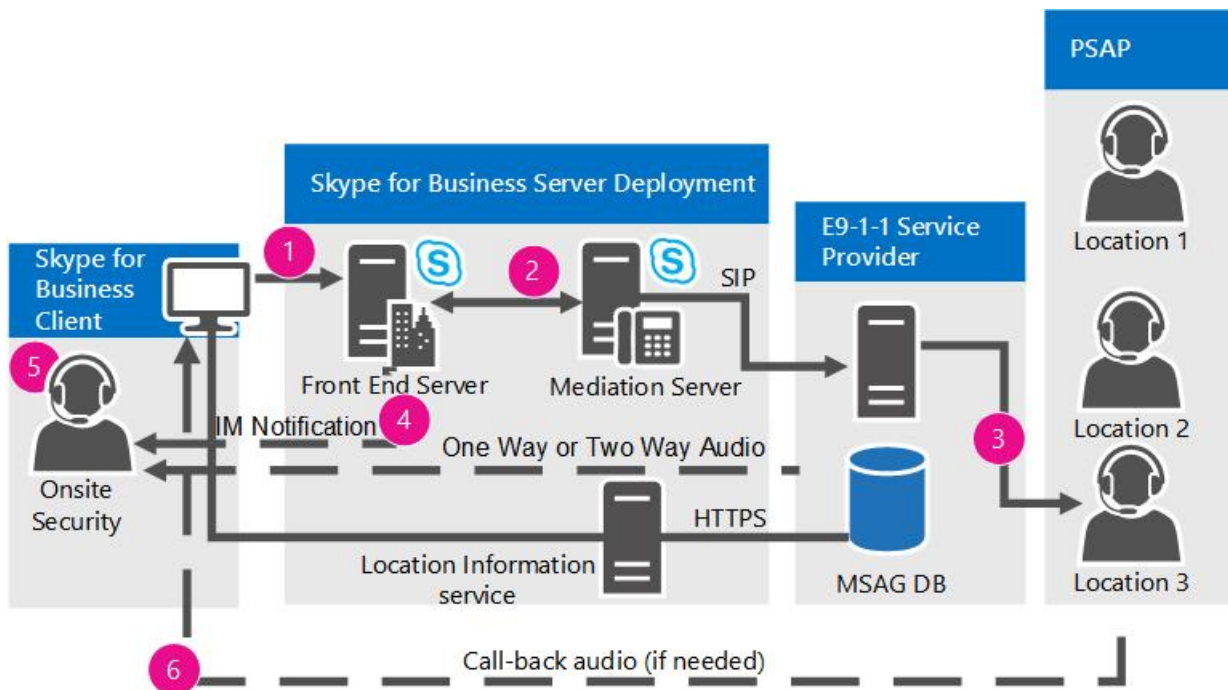
1. The administrator populates the Location Information service database with the network wiremap (tables that map various types of network addresses to corresponding Emergency Response Locations (ERLs)).
2. If you use a SIP trunk E9-1-1 service provider, the administrator validates the civic address portions of the ERLs against a Master Street Address Guide (MSAG) database maintained by the E9-1-1 service provider. If you use an ELIN gateway, the administrator ensures that the PSTN carrier uploads the ELINs to the Automatic Location Identification (ALI) database.
3. During registration or whenever a network change occurs, an internally-connected client sends a location request that contains the client's discovered network addresses to the Location Information service.
4. The Location Information service queries its published records for a location, and, if a match is found, returns the ERL to the client in PIDF-LO format.

## Routing E9-1-1 calls using a SIP trunk

Using a SIP trunk to connect to a qualified E9-1-1 service provider is one way that you can deploy E9-1-1. For details about using an ELIN gateway to connect to a public switched telephone network (PSTN)-based E9-1-1 service provider, see [Routing E9-1-1 Calls by Using an ELIN Gateway](#).

The following diagram shows how an emergency call is routed from Skype for Business Server to the Public Safety Answering Point (PSAP) when you use a SIP trunk and qualified E9-1-1 service provider.

### Routing E9-1-1 calls through a SIP trunk



When an emergency call is placed from a compatible Skype for Business Server client:

1. A SIP INVITE that contains the location, the caller's callback number, and the (optional) Notification URL and conference callback number is routed to Skype for Business Server.
2. Skype for Business Server matches the emergency number and routes the call (based on the **PSTN Usage** value that is defined in the applicable location policy) to a Mediation Server, and from there, over a SIP trunk to the E9-1-1 service provider.
3. The E9-1-1 service provider routes the emergency call to the correct PSAP based on the location that is provided with the call. When the client includes a validated Emergency Response Location (ERL) with the emergency call, the provider automatically routes the call to the appropriate PSAP. If the location was manually entered by the user, the Emergency Call Response Center (ECRC) first verbally verifies the accuracy of the location with the caller before routing the emergency call to the PSAP.
4. If you configured the location policy for notifications, one or more of your organization's security officers are sent a special Skype for Business emergency notification instant message. This message always pops up on the security officers' screen(s) and contains the caller's name, phone number, time, and location, enabling security personnel to quickly respond to the emergency caller by using an instant message or voice.
5. If you configured the location policy for conferencing and it is supported by the E9-1-1 service provider, an internal Security Desk is conferenced into the call with either one-way audio or two-way audio.
6. If the call is broken prematurely, the PSAP uses the callback number to contact the caller directly.

## Routing E9-1-1 calls by using an ELIN gateway

Some partners in the Unified Communications Open Interoperability Program provide qualified Emergency Location Identification Number (ELIN)-capable gateways, which can serve as an alternative to a SIP trunk connection to a qualified E9-1-1 service provider. ELIN gateways support ISDN or Centralized Automatic Message Accounting (CAMA) connectivity to public switched telephone network (PSTN)-based E9-1-1 services. For details about partners who provide ELIN gateways and links to their documentation, see [Infrastructure qualified for Microsoft Lync](#) and [Telephony Infrastructure for Skype for Business](#).

Like SIP trunk connections to E9-1-1 service providers, ELIN gateways also provide the means of routing an emergency call to the caller's most appropriate Public Safety Answering Point (PSAP), but these gateways use an

ELIN as the location identifier. You define ELINs for each Emergency Response Location (ERL) in your organization (for details, see [Manage locations for ELIN gateways in Skype for Business Server](#)).

When you use an ELIN gateway for emergency calls, you use the same Skype for Business Server E9-1-1 infrastructure that you would use for a SIP trunk connection. That is, the Location Information service database provides the location to the Skype for Business client, and the location policy enables the feature and defines the routing. With an ELIN gateway, however, you need to add the ELINs to the Location Information service database and have your PSTN carrier upload them to the Automatic Location Identification (ALI) database.

When a Skype for Business client obtains its location from the Location Information service, the location includes the ELIN. During an emergency call, the ELIN is included with the location sent to the ELIN gateway. The ELIN gateway identifies the call as an emergency call and swaps the calling party's number with the ELIN. The ELIN gateway then routes the call to the PSTN with the ELIN as the calling number. The PSTN E9-1-1 provider looks up the ELIN in the ALI database, which is a companion database to the Master Street Address Guide (MSAG) database. The PSTN then sends the call to the most appropriate PSAP based on the ALI lookup, and the PSAP sends first responders to the caller's location based on the ALI lookup. The calling number is cached on the ELIN gateway for a predefined amount of time for callbacks. During a callback, the PSAP reaches the ELIN gateway, which swaps the ELIN for the caller's direct inward dialing (DID) number.

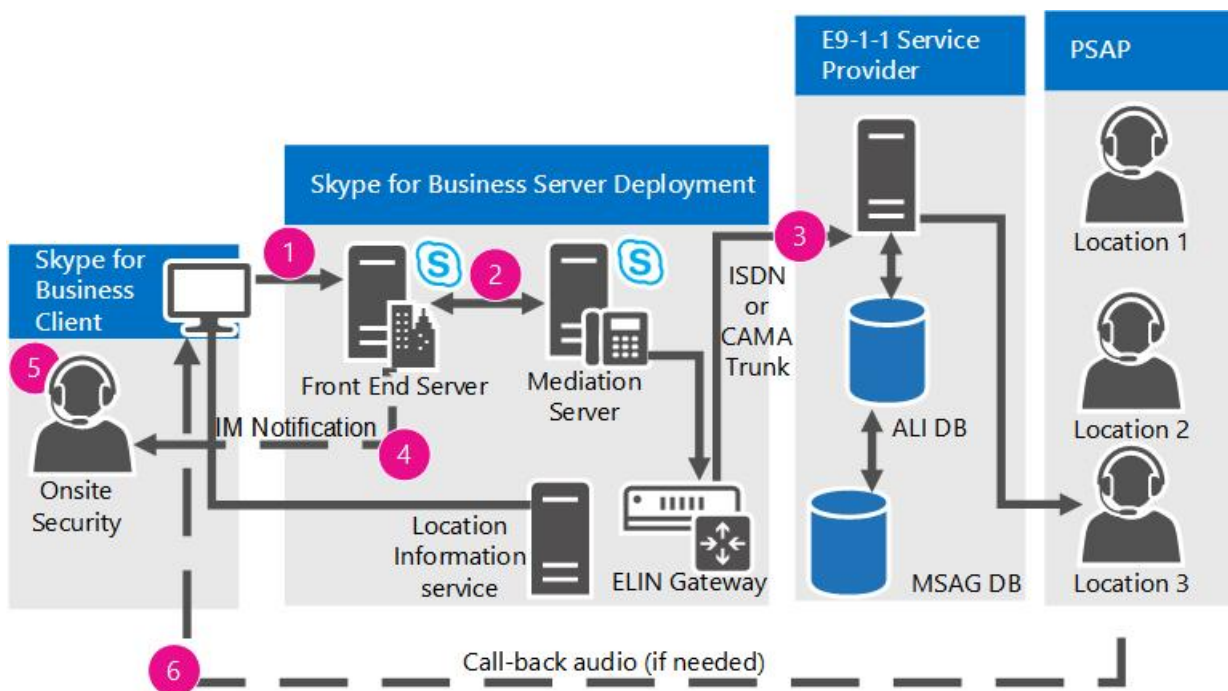
ELIN gateways support emergency calls only from within your organization's network. They do not support emergency calls made from outside your network.

**NOTE**

For details about using a SIP trunk connection for emergency calls, see [Routing E9-1-1 Calls by Using a SIP Trunk](#).

The following diagram shows how an emergency call is routed from Skype for Business Server to the PSAP when you use an ELIN gateway.

**Routing E9-1-1 calls with an ELIN gateway**



1. A SIP INVITE containing the location, the caller's callback number, and the (optional) Notification URL and conference callback number is routed to Skype for Business Server.
2. Skype for Business Server matches the emergency number and then routes the call (based on the **PSTN Usage** value defined in the applicable location policy) to a Mediation Server, and from there to an ELIN

gateway.

3. The ELIN gateway routes the call over an ISDN or CAMA trunk to the PSTN.
4. The PSTN identifies the call as an emergency call and routes it to an E9-1-1 selective router in the network. The E9-1-1 selective router looks up the caller's number in the ALI database to obtain the geographical location. The E9-1-1 selective router sends the call to the most appropriate PSAP based on the location information that was retrieved from the ALI database.
5. If you configured the location policy for notifications, one or more of your organization's security officers are sent a special Skype for Business emergency notification instant message. This message always pops up on the security officers' screen(s) and contains the caller's name, phone number, time, and location, enabling security personnel to quickly respond to the emergency caller by using an instant message or voice.
6. If the call is broken prematurely, the PSAP uses the ELIN to contact the caller directly. The ELIN gateway swaps the ELIN for the caller's DID.

# Define your requirements for emergency calls in Skype for Business Server

5/20/2019 • 2 minutes to read

Summarizes the steps necessary for enabling E9-1-1 in Skype for Business Server Enterprise Voice, depending on whether you have a SIP trunk E9-1-1 service provider or an ELIN gateway.

Before you begin a Skype for Business Server E9-1-1 deployment, you should first be able to answer the questions detailed in the following sections. The planning you need to do depends on the type of E9-1-1 solution that you choose to deploy—a SIP trunk E9-1-1 service provider or an Emergency Location Identification Number (ELIN) gateway. The following table identifies the sections in this planning workbook that you'll need to review for each of those solutions.

## Planning Steps by Type of E9-1-1 Solution

SIP TRUNK SERVICE PROVIDER	ELIN GATEWAY
Define the scope of the E9-1-1 deployment in Skype for Business Server	Define the scope of the E9-1-1 deployment in Skype for Business Server
Define the network elements used to determine location in Skype for Business Server	Define the network elements used to determine location in Skype for Business Server
Enable users for E9-1-1 in Skype for Business Server	Enable users for E9-1-1 in Skype for Business Server
Manage locations for SIP trunk service providers in Skype for Business Server	Manage locations for ELIN gateways in Skype for Business Server
Define the user experience for manually acquiring a location in Skype for Business Server	Define the user experience for manually acquiring a location in Skype for Business Server
Design the SIP trunk for E9-1-1 in Skype for Business Server	Include the security desk in Skype for Business Server
Include the security desk in Skype for Business Server	Plan location policies for Skype for Business Server
Choose an E9-1-1 service provider for Skype for Business Server	Assign location policy scope in Skype for Business Server
Plan location policies for Skype for Business Server	
Assign location policy scope in Skype for Business Server	



# Define the scope of the E9-1-1 deployment in Skype for Business Server

5/20/2019 • 2 minutes to read

Decisions necessary for planning an E9-1-1 deployment in Skype for Business Server Enterprise Voice.

Before you configure Skype for Business for E9-1-1, you need to plan your E9-1-1 deployment. Some of the questions to consider include:

## **What are your organization's policy and legal obligations with regard to E9-1-1?**

E9-1-1 legal requirements for PBXs (called Multi-line Telephone Systems, or MLTS, in E9-1-1 parlance) differ from state to state. You should consult with your legal team to understand the obligations that may apply to your deployment of Skype for Business in your relevant geographies.

## **What areas within your enterprise need to be enabled for E9-1-1?**

You can enable E9-1-1 for the entire enterprise or for selected locations. For example, you may have varying E9-1-1 requirements for offices in different states, or you may want to exclude sites outside the U.S.

## **How will you deploy E9-1-1 to branch sites?**

Voice resiliency is an important concept to understand when deploying E9-1-1 at a branch site. If you have centralized E-9-1-1 SIP trunks and a WAN outage occurs, clients signing in may not be able to obtain a location from Location Information service or to connect to the emergency services service provider. Skype for Business provides several strategies for handling voice resiliency in branch offices, including: having resilient data networks, deploying a SIP trunk at each branch, or pushing emergency calls out to the local gateway during outages. For details, see [Planning for Branch-Site Voice Resiliency](#).

## **Will you enable E9-1-1 for users working outside the network?**

Automatic location acquisition is available only for clients located inside the organization's network, so your organization needs to decide whether it will support E9-1-1 calls made from Skype for Business clients while off-premises. For example, will you enable users to place emergency calls if they are working from home or from a customer site? If a client is located outside the enterprise network, the client can be configured to prompt the user for a location. However, because these user-provided locations cannot be prevalidated against the Master Street Address Guide (MSAG), the emergency services service provider dispatcher will need to confirm the validity of the location verbally with the caller before routing the call to the Public Safety Answering Point (PSAP).

### **NOTE**

Skype for Business clients of users who connect to your organization's network by using VPN can pick up internal IP address information, but because these addresses cannot be used to identify the user's actual location, it is essential that VPN subnets are excluded from the Location Information service.

## **Do you want to provide emergency call routing to sites outside the U.S.?**

You may want to provide emergency routing to areas of your company not served by an emergency services service provider (for example, international locations). To do this, create a new site, and then assign voice policies to the sites that refer to a PSTN usage that routes the call through the local PSTN gateway.

# Define the network elements used to determine location in Skype for Business Server

5/20/2019 • 4 minutes to read

Decisions necessary for planning which network components you will use to map callers to locations for E9-1-1 deployment in Skype for Business Server Enterprise Voice.

If you are setting up your Skype for Business Server infrastructure to support automatic client location detection, you first need to decide which network elements you are going to use to map callers to locations. In Skype for Business Server, you can associate the following Layer 2 and Layer 3 network elements with locations:

- Wireless access point (WAP) Basic Service Set Identification (BSSID) addresses (Layer 2)
- LLDP switch port (Layer 2)
- LLDP switch chassis IDs (Layer 2)
- IP subnets (Layer 3)
- Client MAC addresses (Layer 2)

The network elements are listed in order of precedence. If a client can be located by using more than one network element, Skype for Business Server uses the order of precedence to determine which mechanism to use.

The following sections provide more details for using each network element.

## IMPORTANT

When you use network elements to map callers to locations, it is of utmost importance that you keep the Location Information service database up-to-date. For example, if you add or change a network element, such as adding a WAP, you must delete the old entry and add the new entry in the location database.

## Wireless Access Point

When a client connects to the network wirelessly, the location request uses the BSSID address of the WAP to determine its location. If the client is roaming, the WAP indicated may not be the closest one, and it's even possible to pick up a WAP that is on a different floor of the building. To indicate that the location is approximate, you can prepend the location value with a **[Near]** or **[Closest]** descriptor.

This location method assumes that the BSSID of each WAP is static. However, if your WAP vendor uses dynamically-assigned BSSIDs, the BSSID that is obtained from a WAP could change (this can happen following a WAP configuration change), and wireless clients could be left in a situation where they don't receive a location. To prevent this possibility, you need to populate the Location Information service database with ERLs for all possible BSSID addresses used by each WAP.

## LLDP Ports and Switches

Managed Ethernet switches that support Link Layer Discovery Protocol-Media Endpoint Discover (LLDP-MED) can advertise their identity and port information to LLDP-MED compatible clients, which then can be queried against the location database to provide the location of the device. You can associate ERLs solely on the switch chassis ID, or you can map them down to the port level.

#### NOTE

Skype for Business Server supports using LLDP-MED for determining locations only of Lync Phone Edition devices and Skype for Business clients running on Windows 8. If you need to use switch-level Layer 2 data to determine the location of other wired PC-based Skype for Business Server clients, you need to use the client MAC address method.

## Subnet

Layer 3 IP subnets provide a mechanism supported by all Skype for Business Server clients that can be used to automatically detect client location. Using IP subnets is the easiest location method to configure and manage wired clients. Before you decide to use subnets, however, use the following questions to help determine if the location specificity of the subnet is sufficiently fine to accurately locate a client:

- Do one or more client subnets cover multiple floors?
- Do one or more subnets cover more than one building?
- How much floor space is covered by each client subnet?

If the subnet covers too broad an area, you may need to use another mechanism to locate clients. However, if at all practical, we recommend that customers reorganize their IP subnetting to meet the ERL location specificity requirements rather than incurring the cost and complexity of third-party SNMP-based solutions.

## Client MAC Address

To use a client computer's MAC address to locate a caller, you need managed Ethernet switches, and you must deploy a third-party SNMP solution that can discover the MAC addresses of Skype for Business clients connected to (or through) those switches. The SNMP solution continually polls the managed switches to get the current mappings of the endpoint MAC addresses connected to each port and obtains the corresponding port IDs. During a Skype for Business client's request to the Location Information service, the Location Information service queries the third-party application by using the client's MAC address, and then returns any matching switch IP addresses and port IDs. The Location Information service uses this information to query its published Layer 2 wiremap for a matching record and returns the location to the client. If you use this option, make sure that the switch port identifiers are consistent between the SNMP application and the published location database records.

#### NOTE

Some third-party SNMP solutions can support unmanaged access switches; if the switch that services the Skype for Business client is unmanaged but has an uplink to a managed distribution switch, the managed switch can report back to the SNMP application the MAC addresses of the clients connected to the access switch. This information enables the Location Information service to identify the location of the user. However, it is possible to assign only a single ERL to all ports on the unmanaged switch, so the location specificity is available only at the chassis level of the access switch, not the port level.

# Enable users for E9-1-1 in Skype for Business Server

5/20/2019 • 2 minutes to read

Decisions necessary for the location policy for an E9-1-1 deployment in Skype for Business Server Enterprise Voice, including which users to enable and how to support roaming users.

During client registration, Skype for Business Server uses a location policy to configure the E9-1-1 properties for Enterprise Voice-enabled users. This policy contains the settings that define how E9-1-1 is implemented. For example, the location policy contains information such as the emergency dial string, and whether or not a user is required to manually enter a location if the Location Information service does not automatically provide one. For a complete definition of a location policy, see [Plan location policies for Skype for Business Server](#).

Skype for Business Server can assign a location policy to clients based on subnet, or to users based on a global, per-site, or per-user policy. To help decide how you will enable users, you should first answer the following questions.

## **Do you plan to enable all users, or limit support to specific geographic areas of the enterprise?**

You can assign a location to all users in your enterprise by using a global location policy. However, by assigning a location policy to a Skype for Business Server network site and then adding subnets to the site, you can limit E9-1-1 support to selected locations within the enterprise and specify E9-1-1 routing behavior on a per-site basis.

## **Do you plan to enable individual users through a user policy?**

You can assign location policies directly to specific users or common area phone contact objects if you want to customize their E9-1-1 support.

## **When clients roam outside the network or connect from an undefined subnet, should the clients still be enabled for E9-1-1?**

If users are assigned a global, site, or per-user location policy, they can be required to manually enter a location into the client if the client is not located within a defined subnet or no location has been found by the Location Information service. For details, see [Define the user experience for manually acquiring a location in Skype for Business Server](#).

# Manage locations for SIP trunk service providers in Skype for Business Server

5/20/2019 • 3 minutes to read

Decisions necessary for planning an the location information database, or a similar external database, for an E9-1-1 deployment using SIP trunking providers, in Skype for Business Server Enterprise Voice.

To configure Skype for Business Server to automatically locate clients within a network, you need to either populate the Location Information service database with a network wiremap and publish the locations, or link to an external database that already contains the correct mappings. As part of this process, you need to validate the civic addresses of the locations with your E9-1-1 service provider. For details, see [Configure the Location Database](#) in the Deployment documentation.

You populate the Location Information service database with an Emergency Response Location (ERL), which consists of a civic address and the specific address within a building. The Location Information service **Location** field, which is the specific location within a building, has a maximum length of 20 characters (including spaces). Within that limited length, try to include the following:

- An easy-to-understand name that identifies the location of the 911 caller to help ensure that emergency responders find the specific location promptly when they arrive at the civic address. This location name may include a building number, floor number, wing designator, room number, and so on. Avoid nicknames known only to employees, which might cause emergency responders to go to the wrong location.
- A location identifier that helps users to easily see that their Skype for Business client picked up the correct location. The Skype for Business client automatically concatenates and displays the discovered **Location** and **City** fields in its header. A good practice is to add the street address of the building to each location identifier (for example, "1st Floor "). Without the street address, a generic location identifier such as "1st Floor" could apply to any building in the city.
- If the location is approximate because it's determined by a wireless access point, you can add the word **[Near]** (for example, "Near 1st Floor 1234").

## NOTE

Locations added to the central location database are not available to the client until they are published by using a Skype for Business Server Management Shell command and are replicated to the pool's local stores. For details, see [Publishing the Location Database](#) in the Deployment documentation.

The following sections discuss considerations that you need to take into account when populating and maintaining the location database.

## Populating the Location Database

The following questions can help you determine how to populate the location database.

### What process will you use to populate the location database?

Where does the data exist, and what steps do you need to take to convert the data into the format required by the location database? Will you add locations individually, or in bulk, by using a CSV file?

### Do you have a third party database that already contains a mapping of locations?

By using the Secondary Location Information service option to connect to a third-party database, you can group and manage locations by using an offline platform. A benefit to this approach is that in addition to associating locations to network identifiers, you can associate locations to a user. This means that the Location Information service can return multiple addresses, originating from the Secondary Location Information service, to a Skype for Business client. The user can then choose the most appropriate location.

To integrate with the Location Information service, the third-party database must follow the Lync Server Location Request/Response schema. For details, see "[MS-E911WS]: Web Service for E911 Support Protocol Specification". For details about deploying a Secondary Location Information service, see [Configure a secondary Location Information service in Skype for Business Server](#) in the Deployment documentation.

For details about populating the location database, see [Configure the Location Database](#) in the Deployment documentation.

## Maintaining the Location Database

After you populate the location database, you need to develop a strategy for updating the database as the network configuration changes. The following questions will help you determine how to maintain the location database.

### **How will you update the location database?**

There are several scenarios that require an update to the location database, including adding WAPs, office recabling (resulting in different switch assignments), and subnet expansion. Will you directly update each individual location, or will you perform a bulk update of all the locations by using a CSV file?

### **Will you use an SNMP application to match Lync client MAC addresses to port and switch identifiers?**

If you use an SNMP application, you need to develop a manual process for keeping the switch chassis and port information consistent between the SNMP application and the location database. If the SNMP application returns a chassis IP address or port ID that is not included in the database, the Location Information service will not be able to return a location to the client.

# Manage locations for ELIN gateways in Skype for Business Server

5/20/2019 • 5 minutes to read

Decisions necessary for planning the location information database, or a similar external database, for an E9-1-1 deployment using ELIN gateways, in Skype for Business Server Enterprise Voice.

To have Skype for Business Server automatically provide locations for clients within a network, you need to perform the following tasks:

- Populate the Location Information service database with a network wiremap, and include the Emergency Location Identification Numbers (ELINs) in the CompanyName field.
- Publish the locations so that they are available for clients in your network.
- Upload the ELINs to your public switched telephone network (PSTN) carrier's Automatic Location Identification (ALI) database.

For details about how to perform these tasks, see [Configure the Location Database](#) in the Deployment documentation.

## NOTE

Locations added to the central location database are not available to the client until they have been published by using a Skype for Business Server Management Shell command and are replicated to the pool's local stores. For details, see [Publishing the Location Database](#) in the Deployment documentation.

This section describes things to consider as you plan to update and maintain the location database.

## Planning Emergency Locations

When you use ELIN gateways, you populate the Location Information service database with the civic address, a specific location within a building, and at least one ELIN for each location. During the planning phase, it is a good idea to decide how you want to name the locations and how you want to assign ELINs.

### Planning Location Names

The Location Information service **Location** field, which holds the specific location within a building, has a maximum length of 20 characters (including spaces). Within that limited length, try to include the following:

- An easy-to-understand name that identifies the location of the 911 caller to help ensure that emergency responders find the specific location promptly when they arrive at the civic address. This location name may include a building number, floor number, wing designator, room number, and so on. Avoid nicknames that are known only to employees, which might cause emergency responders to go to the wrong location.
- A location identifier that helps users to easily see that their client picked up the correct location. The Skype for Business client automatically concatenates and displays the discovered **Location** and **City** fields in its header. A good practice is to add the street address of the building to each location identifier (for example, "1st Floor "). Without the street address, a generic location identifier such as "1st Floor" could apply to any building in the city.
- If the location is approximate because it's determined by a wireless access point, you may want to add the

word **[Near]** (for example, "Near 1st Floor 1234").

## Planning ELINs

After you decide how you want to divide your building space into locations, you need to decide how many ELINs to assign to each location. For example, in a multifloor or multitenant building, different areas in the building can be assigned different emergency zones. Typically, each floor in a building is designated as a location. Each location is then assigned one or more ELINs, which are used as the calling number(s) during an emergency call. Contact your PSTN carrier for phone numbers that you can use for ELINs. The following table provides an example of locations for a specific street address.

### Sample Location and ELIN Assignments

BUILDING AREA	LOCATION	ELIN
First floor	1	425-555-0100
Second floor	2	425-555-0111
Third floor	3	425-555-0123

The locations you define should meet the following requirements:

- Comply with local and national/regional regulations in terms of maximum area per location and number of locations per street address.
- Are specific enough to make it easy to locate the emergency caller.

## Populating the Location Database

The following questions will help you determine how to will populate the location database.

### What process will you use to populate the location database?

Where does the data exist, and what steps do you need to take to convert the data into the format required by the location database? Will you add locations individually, or in bulk, by using a CSV file?

### Do you have a third party database that already contains a mapping of locations?

By using the Secondary Location Information service option to connect to a third-party database, you can group and manage locations by using an offline platform. A benefit to this approach is that in addition to associating locations to network identifiers, you can associate locations to a user. This means that the Location Information service can return multiple addresses, originating from the Secondary Location Information service, to a Skype for Business client. The user can then choose the most appropriate location.

To integrate with the Location Information service, the third-party database must follow the Skype for Business Server Location Request/Response schema. For details, see [Web Service for E911 Support Protocol](#). For details about deploying a Secondary Location Information service, see [Configure a secondary Location Information service in Skype for Business Server](#) in the Deployment documentation.

For details about populating the location database, see [Configure the Location Database](#) in the Deployment documentation.

## Maintaining the Location Database

After you populate the location database, you need to develop a strategy for updating the database as the network configuration changes. The following questions will help you determine how to maintain the location database.



**How will you update the location database?**

There are several scenarios that require an update to the location database, including adding wireless access points (WAPs), office recabling (resulting in different switch assignments), and subnet expansion. Will you directly update each individual location, or will you perform a bulk update of all the locations by using a CSV file?

**Will you use an SNMP application to match Skype for Business client MAC addresses to port and switch identifiers?**

If you use an SNMP application, you need to develop a manual process for keeping the switch chassis and port information consistent between the SNMP application and the location database. If the SNMP application returns a chassis IP address or port ID that is not included in the database, the Location Information service will not be able to return a location to the client.

# Define the user experience for manually acquiring a location in Skype for Business Server

5/20/2019 • 2 minutes to read

Planning for roaming users in an E9-1-1 deployment using SIP trunking providers, in Skype for Business Server Enterprise Voice.

If a client is located outside the network, or in an undefined subnet, the user can manually enter a location. But during an emergency call, the call will first be routed to a national/regional E9-1-1 Emergency Call Response Center (ECRC) dispatcher before being routed to a Public Safety Answering Point (PSAP). The ECRC will verbally query the caller for a location and then forward the call to the appropriate PSAP, based on the information provided.

## **Should users be prompted to enter a location when one is not automatically provided by the Location Information service?**

For example, if a client is located in an undefined subnet, at home, in a hotel, or anywhere else outside the network, should the user be required to enter a location?

You can configure the **Location Required** setting in the location policy to define the client behavior. Setting this value to No means that the user will not be prompted for a location. Setting this value to Yes means that the user will be prompted for a location, but can dismiss the prompt. Setting this value to Disclaimer means that the user will be prompted for a location, and will be shown a disclaimer if they try to dismiss the prompt. In all cases, the user can continue to use the client as usual.

When a user manually enters a location, the location is mapped to the MAC address of the default gateway of the client's network, and is stored in a per-user table located on the client. When the user returns to any previously stored location, the Skype for Business client automatically sets itself to that location.

### **NOTE**

You can modify only the current location of your client, but you can also delete any location stored in the local user's table.

# Design the SIP trunk for E9-1-1 in Skype for Business Server

5/20/2019 • 3 minutes to read

Planning your SIP trunking topologies for an E9-1-1 deployment that uses SIP trunking providers, in Skype for Business Server Enterprise Voice.

Skype for Business Server uses SIP trunks to connect an emergency call to the E9-1-1 service provider. You can set up emergency service SIP trunks for E9-1-1 at one central site, at multiple central sites, or at each branch site. However, if the WAN link between the caller's site and the site that hosts the emergency service SIP trunk is unavailable, then a call placed by a user at the disconnected site will need a special phone usage record in the user's voice policy that will route the call to the ECRC through the local public switched telephone network (PSTN) gateway. The same is true if call admission control concurrent call limits are in effect.

There are two ways to implement a SIP trunk in a Skype for Business Server environment:

- Use multihomed Mediation Servers that use their outward-facing publicly-routed interfaces to communicate with the SIP trunk provider.
- Use an on-premises Session Border Controller (SBC) to provide a secure demarcation point between the Mediation Servers and the SIP trunk provider's services.

If you choose the latter method, be sure that the SBC make and model that you choose has been certified and supports passing Presence Information Data Format Location Object (PIDF-LO) location data as part of its SIP INVITE. Otherwise, the calls will arrive at the emergency services service provider stripped of their location information. For details about certified SBCs, see "[Infrastructure Qualified for Microsoft Lync](#)" and "[Telephony Infrastructure for Skype for Business](#)".

E9-1-1 service providers supply you with access to a pair of SBCs for redundancy. You need to make several decisions regarding the Mediation Server topology and call routing configuration. Will you treat both SBCs as equal peers and use round-robin routing for calls between them, or will you designate one SBC as primary and the other as secondary?

For details about deploying a SIP trunk in Skype for Business Server, see [SIP trunking in Skype for Business Server](#). The following questions will help you decide how to deploy the SIP trunks for E9-1-1.

## Should you deploy the SIP trunk over a dedicated leased or a shared internet connection?

It is important that emergency calls always connect. A dedicated line provides a connection that will not be preempted by other traffic on the network, and gives you the ability to implement Quality of Service (QoS). Remember that if you are connecting to emergency services service providers over the public Internet and you need to guarantee the confidentiality of emergency calls, IPSec encryption is required.

## Is your E9-1-1 deployment designed for disaster tolerance?

Because this is an emergency solution, resiliency is important. Deploy your primary and secondary Mediation Servers and SIP trunks in disaster tolerant locations. It is a good idea to deploy your primary Mediation Server closest to the users that it is supporting, and route failover calls through the secondary Mediation Server (located in a different geographic location).

## Should you deploy a separate SIP trunk for each branch office?

Skype for Business Server provides several strategies for handling voice resiliency in branch offices, including: having resilient data networks, deploying a SIP trunk at each branch, or pushing calls out to the local gateway during outages. For details, see [SIP trunking in Skype for Business Server](#).

### **Is call admission control (CAC) enabled?**

Skype for Business Server does not handle emergency calls any differently than an ordinary call. For this reason, bandwidth management, or call admission control (CAC), can have a negative impact on an E9-1-1 configuration. Emergency calls will be blocked or routed to the local PSTN gateway if a CAC is enabled and the configured limit is exceeded on a link where emergency calls are being routed. As indicated earlier in this topic, such calls will not have location data and must be manually routed to the ECRC.

# Include the security desk in Skype for Business Server

5/20/2019 • 2 minutes to read

Planning how to include your organization's security desk in an E9-1-1 deployment, in Skype for Business Server Enterprise Voice.

Your company may require the security desk to become involved in an emergency call. To help decide how to integrate the Security Desk into your E9-1-1 deployment, you should answer the following questions.

## **Do you want the security desk to be notified when there is an emergency call?**

You can configure the location policy so that Skype for Business Server sends instant messaging (IM) alerts to the Skype for Business SIP addresses of one or more security personnel. These alerts contain the name, number, and location of the person placing the emergency call, and facilitate security personnel in assisting with the emergency situation.

## **Do you want to conference the security desk in on each emergency call?**

If supported by the emergency services service provider, you can configure the location policy to include a callback number with each emergency call. This number is then used by the provider to conference your organization's security personnel into emergency calls. This conferencing can be configured in the location policy to be one-way (listen-only) or two-way (bidirectional).

### **NOTE**

If desired, you can configure different emergency personnel for each location policy. This allows you to customize the response for different areas within your company, or create different behavior for emergency calls that originate from inside as opposed to outside the network. You can use distribution groups to specify the personnel you want to notify.

# Choose an E9-1-1 service provider for Skype for Business Server

5/20/2019 • 2 minutes to read

Choosing your service provider for an E9-1-1 deployment in Skype for Business Server Enterprise Voice.

The E9-1-1 service provider routes emergency calls originating from Skype for Business Server to the correct Public Safety Answering Point (PSAP) based on the location information contained within the call.

To support E9-1-1 as part of a Skype for Business Server deployment, you must obtain E9-1-1 routing service from a Lync Open Interoperability Program qualified E9-1-1 service provider. Choose the provider that best fits your organizational requirements.

To see the list of E9-1-1 routing services for Lync, see [E-911 Services qualified for Lync](#).

# Plan location policies for Skype for Business Server

5/20/2019 • 4 minutes to read

Read this topic to learn how to plan location policies for an enhanced emergency services (E9-1-1) deployment in Skype for Business Server Enterprise Voice.

## NOTE

Skype for Business Server now supports the configuration of multiple emergency numbers for a client. If you want to configure multiple emergency numbers, you must follow the information in [Plan for multiple emergency numbers in Skype for Business Server](#) and [Configure multiple emergency numbers in Skype for Business](#).

You create location policies by using the Skype for Business Control Panel or by using the `New-CsLocationPolicy` cmdlet. For more information, see [Create location policies in Skype for Business Server](#).

Each location policy contains the following information:

### Enable Enhanced 9-1-1

When this value is enabled, the client is enabled for enhanced emergency services (E9-1-1). When a client registers, it attempts to acquire a location from the Location Information service and will include the location information as part of an emergency call.

### Location

This setting is used only when **Enable Enhanced 9-1-1** is enabled.

You can configure the **Location** setting to define the client behavior as follows:

- Setting the value to **No** means that the user will not be prompted for a location.
- Setting the value to **Yes** means that the user will be prompted for a location, but can dismiss the prompt.
- Setting the value to **Disclaimer** means that the user will be prompted for a location and also will be shown a disclaimer if they try to dismiss the prompt. In all cases, the user can continue to use the client.

## NOTE

The disclaimer text will not appear if a user manually entered a location before being enabled for E9-1-1. Updates to the disclaimer text will not be viewed by users that have already viewed the disclaimer.

### Enhanced Emergency Service Disclaimer

This setting specifies the disclaimer that users see if they dismiss the prompt for a location. In Skype for Business Server, you can use location policy to set different disclaimers for different locales or different sets of users.

### Emergency Dial String (E9-1-1 dial number)

This dial string (less the leading "+", but including any normalization done by the user's Dial Plan) signifies that a call is an emergency call. The **Emergency Dial String** causes the client to include location and callback information with the call.

#### **NOTE**

If your organization does not use an external line access prefix, you do not need to create a corresponding Dial Plan normalization rule that adds a "+" to the 911 string prior to sending the call to Outbound Routing on a server running Skype for Business Server; the "+" will be automatically prepended by the Skype for Business client as a result of the location policy. However, if your site uses an external access prefix, you need to add a normalization rule to the applicable Dial Plan policy that strips the external access prefix and adds the "+". For example, if your location uses an external access prefix of 9 and a user dials 9 911 to place an emergency call, the client will use its Dial Plan policy to normalize this to +911 before the dialed number is evaluated by the routes in the caller's location profile.

### **Emergency Dial String Masks (E9-1-1 dial mask)**

A semicolon-separated list of dial strings that is translated into the specified **Emergency Dial String**. For example, you may want to add 112, which is the emergency service number for most of Europe. A visiting Skype for Business user from Europe may not know that 911 is the U.S. emergency number, but they can dial 112 and get the same result. As with the Emergency Dial String, do not include a "+" before each number, and if you use external line access codes, be sure there are normalization rules in the user's Dial Plan policy to strip off the access code digit.

### **PSTN usage**

The name of the PSTN Usage that contains the routing paths that determine which SIP trunk, PSTN gateway, or ELIN gateway emergency calls will go to.

#### **NOTE**

Only one usage can be assigned to a location policy. This PSTN Usage overrides the PSTN Usages assigned to the user's voice policy, but applies only to calls placed to the Emergency Dial String or to one of the Emergency Dial String Masks.

### **Notification URI**

Specifies one or more SIP URIs of the security personnel who receive an instant messaging (IM) notification when an emergency call is placed. Distribution groups are supported.

### **Conference URI**

Specifies a direct inward dialing (DID) number (typically, a security desk number) that should be conferenced in when an emergency call is placed.

### **Conference Mode**

Specifies if the conference URI will be conferenced into the emergency call by using one-way or two-way communication.

### **Location Refresh Interval**

Specifies the amount of time (in hours) between client requests for a location update from the Location Information service. The value can be set to any value between 1 and 12. The default value is 4.



# Assign location policy scope in Skype for Business Server

5/20/2019 • 2 minutes to read

Planning location policies for an E9-1-1 deployment in Skype for Business Server Enterprise Voice.

As with other Skype for Business Server policies, location policies can be assigned at multiple scope levels: global, site, and user. However, the scope of user-level location policies behaves a bit differently than with other Skype for Business Server policies. Not only can per-user location policies be applied to endpoint objects (such as Users and Common Area Phone contact objects), they can also be applied to Skype for Business Server network sites.

Network sites are groupings of client subnets associated with a geographical location (but may not necessarily be all subnets in an entire central site or branch site). Any clients connected to the subnets in a network site automatically pick up the location policy assigned to that network site. In cases where a user-level location policy is assigned both to a user and to a network site, the network site-based location policy overrides any per-user policy setting.

Each network site has a location policy assigned to it, and each policy will have different PSTN Usages, Notification URIs, and Conference URIs values assigned to it.

## NOTE

The reason for this special policy scoping behavior is so that when a user homed on a pool at one office site visits another site and has to make an emergency call, the E9-1-1 call routing settings appropriate to that network site will apply no matter what pool or site the user is assigned to.

# Plan for multiple emergency numbers in Skype for Business Server

5/20/2019 • 6 minutes to read

Read this topic to learn how to plan for multiple emergency numbers in Skype for Business Server.

Skype for Business Server now supports the configuration of multiple emergency numbers for a client. Multiple emergency numbers is a new feature introduced in the June 2016 Cumulative Update. While the United States has a single emergency number, 911, many countries support multiple emergency numbers. The United Kingdom, for example, supports both 999, the emergency number specific to the United Kingdom, and 112, the emergency number for the European Union.

This feature is also useful for health care providers within the United States who want to have roaming support for multiple code blue emergency numbers.

## Multiple emergency numbers and location policies

You configure emergency calling by creating location policies that define how emergency calling will be implemented. You use the location policy to define what number constitutes an emergency call—for example, 911 in the United States; 999 and 112 in the United Kingdom. The location policy determines whether a user is enabled for emergency calling, and if so what the behavior is of an emergency call. You can also define whether corporate security should be automatically notified, and how the call should be routed.

For more information about defining and modifying a location policy, see [Plan location policies for Skype for Business Server](#) and [Create location policies in Skype for Business Server](#). These topics describe concepts about location policies; however, you must follow the instructions in [Configure multiple emergency numbers in Skype for Business](#) to configure multiple emergency numbers.

When planning for multiple emergency numbers, keep the following in mind:

- With the June 2016 Cumulative Update, you can define up to 5 emergency numbers for a given location policy. With the November 2016 Cumulative Update, this number increases to 100.

### NOTE

If you have not yet upgraded to the November 2016 Cumulative Update, see [Updates to Skype for Business Server 2015](#).

- For each emergency number, you can specify zero or more emergency dial masks, which are unique to a given location policy.

A dial mask is a number that you want to translate into the value of the emergency dial number value when it is dialed. For example, assume you enter a value of 212 in this field and the emergency dial number field has a value of 911. When a user dials 212, the number will be translated to 911. This allows for alternate emergency numbers to be dialed and still have the call reach emergency services (for example, if someone from a country or region with a different emergency number attempts to dial that country or region's number rather than the number for the country or region they are currently in). You can define multiple emergency dial masks by separating the values with semicolons. For example, 212;414. The string limit for a dial mask is 100 characters. Each character must be a digit 0 through 9.

- Each location policy has a single public switched telephone network (PSTN) usage that is used to determine

which voice route is used to route emergency calls from clients using this policy. The usage can have a unique route per emergency number.

- If a location policy has both the EmergencyNumbers and DialString parameters defined, and the client supports multiple emergency numbers, then the emergency number takes precedence. If the client does not support multiple emergency numbers, then the emergency dial string is used.
- For information about which Skype for Business and Lync clients support receiving multiple emergency numbers, dial masks, and public switched telephone network (PSTN) usages, see [Client support](#).

**NOTE**

You cannot configure multiple emergency numbers by using the Skype for Business Control Panel. You must use PowerShell to configure multiple emergency numbers.

Before you configure multiple emergency numbers, keep the following in mind:

- To configure multiple emergency numbers, you must use the New-CsEmergencyNumber cmdlet, and you must define location policies that support more than one emergency number by specifying the EmergencyNumbers parameter with the [New-CsLocationPolicy](#) and [Set-CsLocationPolicy](#) cmdlets.
- If you have existing numbers defined using the Set-CsLocationPolicy or New-CsLocationPolicy cmdlet with the EmergencyDialString and EmergencyDialMask parameters, the values specified with the EmergencyNumbers parameter will take precedence over the old values. That is, the values for the EmergencyDialString and EmergencyDialMask parameters will be ignored.
- If you have existing numbers defined using the Set-CsLocationPolicy or New-CsLocationPolicy cmdlet with the EmergencyDialString and EmergencyDialMask parameters, *and you do not configure new emergency numbers*, the existing numbers will continue to be used.
- For the multiple emergency numbers feature to work, the client versions you are running must be able to support the new feature. Older clients will continue to use the old values specified by the Set-CsLocationPolicy or New-CsLocationPolicy cmdlets with the EmergencyDialString and EmergencyDialMask parameters.
- If the users will be dialing a number that matches the dial string, then no dial mask is required. For example, if the number a user dials is 911, then the dial string is 911 and no mask is required.

For more information about configuring multiple emergency numbers, see [Configure multiple emergency numbers in Skype for Business](#).

The following table shows example location policies (for purposes of the example, not all attributes are shown):

LOCATION POLICY NAME	E911 ENABLED	EMERGENCY DIAL STRING	DIAL MASK	EMERGENCY NUMBERS	PSTN USAGE	LOCATION REQUIRED
United States	Yes	911	112;999		USEmergency	Yes
US-Hospital	Yes	911	450	911 450	SeattleEmergency	Yes
London	Yes	999	144	999-144 112- 911;117;118	GBEmergency	No

LOCATION POLICY NAME	E911 ENABLED	EMERGENCY DIAL STRING	DIAL MASK	EMERGENCY NUMBERS	PSTN USAGE	LOCATION REQUIRED
India	Yes			100-911 101 102	IndiaEmergency	No

**United States** —There is no requirement for multiple emergency numbers. In the United States, you use the old Emergency Dial String and Dial Mask configurations.

**US-Hospital** —There is a requirement not to mask "450". For clients that do not yet support multiple emergency numbers, you can use the old Emergency Dial String and Dial Mask configurations. For clients that support multiple emergency numbers, you can define an emergency number for both "911" and "450" instead of masking 450.

**London** —For clients that do not yet support multiple emergency numbers, you can use the old Emergency Dial String and Dial Mask configurations. For clients that support multiple emergency numbers, you can define an emergency number for both "999" and "112" with masks for each.

**India** —All deployed clients support multiple emergency numbers. In India, you only need to configure multiple emergency numbers.

## Client support

The following table shows client support for multiple emergency numbers. Microsoft will continue to test and release support for additional clients. Please check back often.

WINDOWS	VERSION
<b>Click-to-Run</b>	CC (Current Channel) released on May 10, 2016 - Version 1604 (Build 6868.2062)
	FRDC (First Release Current Channel) released on June 14, 2016 - Version 1605 (Build 6965.2058)
	DC (Deferred Channel) released on October 11, 2016 - Version 1605 (Build 6965.2092)
<b>MSI</b>	June 7 update - <a href="https://support.microsoft.com/en-us/kb/3115087">https://support.microsoft.com/en-us/kb/3115087</a>
<b>Mac and iOS</b>	<b>Version</b>
	Skype for Business Mac client version 16.9 Skype for Business iOS client version 6.16
<b>Android</b>	<b>Version</b>
	Skype for Business Android client version 6.17
<b>Lync Phone Edition</b>	<b>Version</b>
	Aastra 6721ip and Aastra 6725ip telephones - September 2016 cumulative update (Build 7577.4512) - <a href="https://support.microsoft.com/en-us/kb/3194831">https://support.microsoft.com/en-us/kb/3194831</a>

WINDOWS	VERSION
	HP 4110 and HP 4120 telephones - September 2016 cumulative update (Build 7577.4512) - <a href="https://support.microsoft.com/en-us/kb/3194832">https://support.microsoft.com/en-us/kb/3194832</a>
	Polycom CX500, Polycom CX600, and Polycom CX3000 telephones - September 2016 cumulative update (Build 7577.4512) - <a href="https://support.microsoft.com/en-us/kb/3194833">https://support.microsoft.com/en-us/kb/3194833</a>

# Plan for media bypass in Skype for Business

5/20/2019 • 8 minutes to read

Decisions necessary for planning for media bypass in Skype for Business Server Enterprise Voice. Includes interoperation with call admission control (CAC).

Media bypass refers to removing the Mediation Server from the media path whenever possible for calls whose signaling traverses the Mediation Server.

Media bypass can improve voice quality by reducing latency, needless translation, possibility of packet loss, and the number of points of potential failure. Scalability can be improved, because elimination of media processing for bypassed calls reduces the load on the Mediation Server. This reduction in load complements the ability of the Mediation Server to control multiple gateways.

Where a branch site without a Mediation Server is connected to a central site by one or more WAN links with constrained bandwidth, media bypass lowers the bandwidth requirement by allowing media from a client at a branch site to flow directly to its local gateway without first having to flow across the WAN link to a Mediation Server at the central site and back.

By relieving the Mediation Server from media processing, media bypass may also reduce the number of Mediation Servers that an Enterprise Voice infrastructure requires. As a general rule, enable media bypass wherever possible.

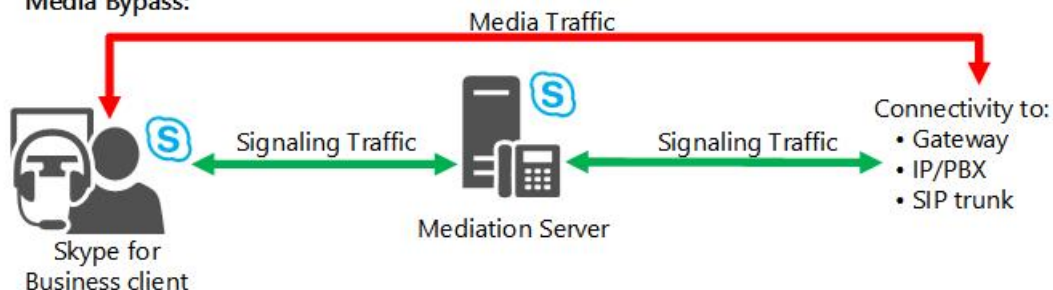
The following figure shows basic media and signaling pathways in topologies with and without media bypass.

## Media and signaling pathways with and without media bypass

### No Media Bypass:



### Media Bypass:



Media bypass is useful when you want to minimize the number of Mediation Servers deployed. Typically, a Mediation Server pool will be deployed at a central site, and it will control gateways at branch sites. Enabling media bypass allows media for public switched telephone network (PSTN) calls from clients at branch sites to flow directly through the gateways at those sites. Skype for Business Server outbound call routes and Enterprise Voice policies must be properly configured so that PSTN calls from clients at a branch site are routed to the appropriate gateway.

Wi-Fi networks typically experience more packet loss than wired networks. Recovery from this packet loss is not typically something that can be accommodated by gateways. Therefore, we recommend that you evaluate the quality of a Wi-Fi network before determining whether bypass should be enabled for a wireless subnet. There is a tradeoff in latency reduction versus recovery from packet loss to consider, as well. RTAudio, a codec which is available for calls that do not bypass the Mediation Server, is better suited for handling packet loss.

## Planning your media bypass deployment

After your Enterprise Voice structure is in place, planning for media bypass is straightforward.

- If you have a centralized topology without WAN links to branch sites, you can enable global media bypass, because fine-tuned control is unnecessary.
- If you have a distributed topology that consists of one or more network regions and their affiliated branch sites, determine the following:
  - Whether your Mediation Server peers are able to support the capabilities required for media bypass.
  - Which sites in each network region are well-connected.
  - Which combination of media bypass and call admission control is appropriate for your network.

When you enable media bypass, a unique bypass ID is automatically generated for a network region, and for all network sites without bandwidth constraints within that region. Sites with bandwidth constraints within the region and sites connected to the region over WAN links with bandwidth constraints are each assigned their own unique bypass IDs.

When a user makes a call to the PSTN, the Mediation Server compares the bypass ID of the client subnet with the bypass ID of the gateway subnet. If the two bypass IDs match, media bypass is used for the call. If the bypass IDs do not match, media for the call must flow through the Mediation Server.

When a user receives a call from the PSTN, the user's client compares its bypass ID to that of the PSTN gateway. If the two bypass IDs match, media flows directly from the gateway to the client, bypassing the Mediation Server.

Only Lync 2010 or newer clients and devices support media bypass interactions with a Mediation Server.

### IMPORTANT

In addition to enabling media bypass globally, you must enable media bypass individually on each PSTN trunk. If bypass is enabled globally, but is not enabled for a particular PSTN trunk, media bypass will not be invoked for any calls involving that PSTN trunk. In addition, when media bypass is set to **Use Site and Region Information**, you must associate all routable subnets with the sites in which they are located. If there are routable subnets within a site for which bypass is not wanted, these subnets should be grouped within a new site before you enable media bypass. Doing so will assure that the unroutable subnets are assigned a different bypass ID.

## Media bypass modes

You must configure media bypass both globally and for each individual PSTN trunk. When enabling media bypass globally, you have two choices: **Always Bypass** and **Use Site and Region Information**.

As the name suggests, **Always Bypass** means that bypass will be attempted for all PSTN calls. **Always Bypass** is used for deployments where there is no need to enable call admission control, nor is there a need to specify detailed configuration information regarding when to attempt media bypass. Furthermore, **Always Bypass** is used when there is full connectivity between clients and PSTN gateways. In this configuration, all subnets are mapped to one and only one bypass ID, which is computed by the system.

With **Use Site and Region Information**, the bypass ID associated with site and region configuration is used to make the bypass decision. This configuration provides the flexibility to configure bypass for most common topologies, as it gives you fine-grained control over when bypass happens, in addition to supporting interactions with call admission control (CAC). The system tries to ease your task by automatically assigning bypass IDs as follows.

- The system automatically assigns a single unique bypass ID to each region.
- Any site connected to a region over a WAN link without bandwidth constraints inherits the same bypass ID as the region.
- A site associated with the region over a WAN link with constrained bandwidth is assigned a different bypass ID from that of the region.
- Subnets associated with each site inherit the bypass ID for that site.

## Media bypass and call admission control

Media bypass and call admission control (CAC) work together to manage bandwidth control for call media. Media bypass facilitates media flow over well-connected links; CAC manages traffic on links with bandwidth constraints. Because Media Bypass and CAC are mutually exclusive, you must be mindful of one when planning for the other. The following combinations are supported:

- CAC and Media Bypass are both enabled. Media Bypass must be set to **Use Site and Region Information**. This site and region information is the same as that used for CAC.

If you enable CAC, you cannot select **Always Bypass**, and vice-versa, because the two configurations are mutually exclusive. That is, only one of the two will apply to any given PSTN call. First, a check is made to determine if media bypass applies to the call. If it does, then CAC is not used. This makes sense, because if a call is eligible for bypass, it is by definition using a connection where CAC is not needed. If bypass cannot be applied to the call (that is, if the client's and gateway's bypass IDs do not match), then CAC is applied to the call.

- CAC not enabled and Media Bypass set to **Always Bypass**.

In this configuration, both client and trunk subnets are mapped to one and only one bypass ID, which is computed by the system.

- CAC not enabled and Media Bypass set to **Use Site and Region Information**.

Where **Use Site and Region Information** is enabled, bypass determination works essentially the same way, regardless of whether CAC is enabled or not. That is, for any given PSTN call, the client's subnet is mapped to a particular site, and the bypass ID for that subnet is extracted. Similarly, the gateway's subnet is mapped to a particular site, and the bypass ID for that subnet is extracted. Only if the two bypass IDs are identical will bypass happen for the call. If they are not identical, media bypass will not occur.

Even though CAC is disabled globally, bandwidth policy needs to be defined for each site and link if you want to use site-and-region configuration to control the bypass decision. The actual value of the bandwidth constraint or its modality doesn't matter. The ultimate goal is to have the system automatically calculate different bypass IDs to associate with different locales that are not well connected. Defining a bandwidth constraint by definition means a link is not well connected.

- CAC is enabled and media bypass is not enabled. This would apply only where all gateways and IP-PBXs are not well connected or do not meet other requirements for media bypass. For details about requirements for media bypass, see [Requirements for Media Bypass](#).

## Technical requirements



For each call to the PSTN, the Mediation Server determines whether media from the Skype for Business endpoint of origin can be sent directly to a Mediation Server peer without traversing the Mediation Server. The peer can be a PSTN gateway, IP-PBX, or Session Border Controller (SBC) at an Internet telephony service provider (ITSP) that is associated with the trunk between the Mediation Server where the call is routed.

Media bypass can be employed when the following requirements are met:

- A Mediation Server peer must support the necessary capabilities for media bypass, the most important being the ability to handle multiple forked responses (known as "early dialogs"). Contact the manufacturer of your gateway or PBX, or your ITSP, to obtain the value for the maximum number of early dialogs that the gateway, PBX, or SBC can accept.
- The Mediation Server peer must accept media traffic directly from Skype for Business endpoints. Many ITSPs allow their SBC to receive traffic only from the Mediation Server. Contact your ITSP to determine whether its SBC accepts media traffic directly from Skype for Business endpoints.
- Skype for Business clients and a Mediation Server peer must be well connected, meaning that they are either located in the same network region or at network sites that connect to the region over WAN links that have no bandwidth constraints

# Plan for private telephone lines with Skype for Business

5/20/2019 • 5 minutes to read

Planning for private (secondary) telephone lines in Skype for Business Server Enterprise Voice.

Skype for Business Server enables you to give users a second, private telephone line in addition to their primary telephone line. Private telephone lines are often assigned to executives and others who want an unlisted telephone number at which they can be reached directly.

Private telephone lines can only be configured with the Skype for Business Server Management Shell. You cannot configure private telephone lines with the Skype for Business Server Control Panel. Private telephone lines should be configured only in deployments of Skype for Business Server and not in mixed deployments.

## Characteristics of Private Telephone Lines

Although the concept of a second, private telephone line is fundamentally simple, it is important to understand the characteristics of private lines and the ways in which they are similar to and different from users' primary telephone lines.

### General Characteristics of Private Telephone Lines

- A user can have only one private telephone line.
- A user with a private telephone line has only one voice mailbox and receives missed call notifications at a single email address.
- A user with a private telephone line does not have a second SIP address, and a second, private telephone line does not give a user a second presence on the network (such as a second instant messaging identity).
- Private telephone lines are available for on-premises deployments only. They are not available with hosted deployments of Skype for Business Server.

### How Private Telephone Lines Differ from Primary Telephone Lines

- The telephone numbers for private telephone lines do not appear in the telephone directories or Contacts lists that are derived from Active Directory Domain Services.
- None of the following features are available with a private telephone line: call forwarding, team call, delegation, team ring, Group Call Pickup, and Response Group application.
- Calls to a private telephone line have a special ring, and the system notification for the call tells the user that the incoming call is on his or her private line.
- Calls to the private telephone line always ring through. They do not follow "do not disturb" rules.
- Private telephone lines are inbound only and cannot be used to make outgoing calls. When a user with a private telephone line makes a call, the call originates from the user's primary telephone line and does not hide the user's name or the user's primary telephone number from the person called.

### How Private Telephone Lines Are Similar to Primary Telephone Lines

- Unanswered calls to a private telephone line are routed to the same voice mail inbox as for the primary telephone line (if voice mail is enabled).
- Call park and call pickup work with private telephone lines in exactly the same manner as they do with the

user's primary telephone line.

- When simultaneous ringing is enabled on a user's primary telephone line, it is also enabled on the private telephone line.
- The telephone number for a private telephone line is recorded in the call detail record in the same manner as the telephone number for a user's primary telephone line, but with an indication that it is a private telephone number.
- After a user answers a call on a private telephone line, the call is treated the same as a call on the user's primary telephone line. For example, if a user who receives a call on a private telephone line forwards the call or invites others to a conference call, the user's name appears in Skype for Business, and the telephone number for the user's primary telephone line appears in caller ID.
- A user can deflect a call (redirect the call to another destination, such as a mobile phone or home phone, before answering) from the private telephone line in the same manner as with a primary telephone line.

#### NOTE

When a call to a private line is routed to an alternate telephone number, the telephone number for the private telephone line is made available to the alternate telephone number and can be displayed in the logs for that number.

#### NOTE

Calls from a conference to the private telephone line will not have a *private-line* indication in the incoming system notification.

## Administering Private Telephone Lines

In addition to the technical aspects of creating and managing private telephone lines, you will need to establish administrative procedures for them. This includes determining policies for who in the organization is eligible for a private line, creating and maintaining lists of people and their telephone lines, possibly creating a private telephone directory for executives, arranging for user training, and related tasks.

#### NOTE

The private telephone line is stored in Active Directory as an msRTCSIP-PrivateLine attribute on the user object. By default any member of the Authenticated Users group has read access to this attribute.

### Assigning Telephone Numbers

Accounts for new users who need private telephone lines are created in the same manner as accounts without private telephone lines, using Skype for Business Server Control Panel or Skype for Business Server Management Shell.

Use the **Set-CsUser** cmdlet in the Skype for Business Server Management Shell to assign a telephone number to a private telephone line for a user, for example, **Set-CsUser -Identity "sip:joe@contoso.com" -PrivateLine "Tel:+14255551212"**.

Telephone numbers for private telephone lines can be between 3 and 15 numbers in length and must be preceded with the "TEL:" prefix. They can have any area code and any country/region code as long as your organization has direct inward dialing for that area code and country/region code.

For details about cmdlets and Skype for Business Server Management Shell, see the Skype for Business Server Management Shell documentation.

### **Private Telephone Lines in Mixed Deployments**

Private telephone lines should be configured only for deployments of Skype for Business Server or Lync Server 2013. In a deployment in which there are servers running earlier versions of Lync Server, when a user on earlier version attempts to call a private telephone line, routing of the call fails because the server cannot perform a reverse number lookup on a private telephone line.

# Plan for Location-Based Routing in Skype for Business

5/20/2019 • 18 minutes to read

Planning for location-based routing in Skype for Business Server Enterprise Voice, including interaction with simultaneous ringing and delegation, and supported scenarios for location-based routing.

Location-Based Routing makes it possible to restrict the routing of calls between VoIP endpoints and PSTN endpoints based on the location of the parties in the call. Location-Based Routing is a call management feature that controls how calls are routed by Skype for Business Server. It enforces call authorization rules on whether calls can be routed to PBX or PSTN endpoints based on the Skype for Business caller's geographic location.

Location-Based Routing introduces a new set of rules that modifies the routing of national and international PSTN calls to prevent toll bypass. Location-Based Routing provides the flexibility to scope these rules to specific regions, specific gateways or to specific set of users only.

The following scenarios illustrate the main types of restrictions Location-Based Routing can enforce:

- Egress calls - Location-Based Routing can enforce outgoing calls to egress to a PSTN gateway that is located in the same region as where the caller is to prevent PSTN toll bypass, which prevents calls to egress to a PSTN gateway located in a different region as the caller.
- Ingress calls - Location-Based Routing can prevent incoming PSTN calls to ring Skype for Business endpoints if the PSTN gateway routing the incoming call is not located in the same region as the called Skype for Business user.
- Unknown regions - Location-Based Routing restricts incoming and outgoing PSTN calls to and from users that are located in undetermined locations (i.e. remote users connecting from the Internet or located in unknown regions).
- International regions - Location-Based Routing enforces routing of outgoing calls through international PSTN gateways if a gateway local to the user's location cannot be found.

## Guidance for where to apply Location-Based Routing

Location-Based Routing depending on the situation can be applied at the user's endpoint network site location or at the PSTN gateway's network site location. This topic provides guidance on how Location-Based Routing is applied.

### **Applying Location-Based Routing at the user's location**

Location-Based Routing leverages the same network regions, sites and subnets as defined in Skype for Business Server used by E9-1-1, CAC and Media Bypass to apply call routing restrictions to prevent PSTN toll bypass. A user's location is determined by the IP subnet of the user's Skype for Business endpoint(s) are connected from. Each IP subnet is associated to a network site, which are aggregated into network regions defined by the administrator. Location-Based Routing is enforced based on the user's network site.

Location-Based Routing rules are applied on a per network site basis, meaning that a given set of rules will be applied to all endpoints enabled for Location-Based Routing that are located within the same network site. Administrators can apply Location-Based Routing to network sites that require it.

Voice routing policies can be defined on a per network site basis to define a particular PSTN gateway that should be used by all users located in the network site to call PSTN phone numbers. Such voice routing policies will take

precedence over the routing defined by the user's voice policy when the user is located in a network site enabled for Location-Based Routing, and it will prevent the routing of calls via other PSTN gateways that are enabled for Location-Based Routing. When a Skype for Business user places a PSTN call, the user's voice policy determines whether the user can be authorized to place the call. If the user's voice policy allows the user to place the call, Location-Based Routing determines which PSTN gateway the call should egress from. Location-Based Routing makes this determination based on the user's location.

A user location can be categorized in the following ways:

- The user is located in a known network site enabled for Location-Based Routing and his DID (Direct Inward Dial) number terminates on a PSTN gateway placed in the same network site (i.e. office). The routing of outbound calls will be through the voice routing policy of the network site in which the user is located. Incoming PSTN calls to the user are routed to endpoints that are located in the same network site as the PSTN gateway.
- The user is located in a known network site that is in different from the network site where the PSTN gateway is located. (i.e. the user traveled to another corporate office). The routing of outbound calls will be using the voice routing policy of the network site in which the user is located. Incoming PSTN calls to the user will not be routed to endpoints that are located in different sites than the PSTN gateway to prevent PSTN toll bypassing.
- When a user is located in a network site that is unknown to the Skype for Business Server deployment, the routing of outbound calls will be based on the voice policy assigned to the user to PSTN gateways not bound to Location-Based Routing restrictions. Incoming PSTN calls will not be routed to endpoints that are located in unknown network sites to prevent PSTN toll bypassing.

### **Applying Location-Based Routing at the PSTN gateway's location**

Calls routed via PSTN gateways and PBXs might require Location-Based Routing restrictions depending on the location of such systems. Location-Based Routing can be enabled at the granularity on a per trunk basis.

Location-Based Routing introduces the following set of rules when enabled on a trunk:

- When Location-Based Routing is enabled on a per trunk basis, the rules define on that trunk will be applied only to calls routed through that trunk.
- To prevent PSTN tolls bypass where calls originate from a network site different than the network site where the PSTN gateway is located, Location-Based Routing introduces the association of a network site to a given trunk. This defines the network site that allows calls to be routed to a given trunk.

Trunks can be enabled for Location-Based Routing in two ways:

- The trunk is defined for a PSTN gateway that egresses calls to the PSTN. Incoming calls routed by a trunk of this type will be routed only to endpoints located within the same network site as the trunk.
- The trunk is defined for a Mediation Server peer that doesn't egress calls to the PSTN and services users with legacy phones in a static locations (i.e. PBX phones). For this particular configuration, all incoming calls routed by a trunk of this type will be considered to be originating from the same network site as the trunk. Calls from PBX users will have the same Location-Based Routing enforcement as Skype for Business users who are located in the same network site as the trunk. If two PBX systems located in separate network sites are connected through Skype for Business Server, Location-Based Routing will allow routing from one PBX endpoint in one network site to another PBX endpoint in the other network site. This scenario will not be blocked by Location-Based Routing. In addition to this scenario and in a similar way as a Skype for Business user in the same location, endpoints connected to a Mediation Server peer with this configuration will be able to make or receive calls to and from other Mediation Server peer that do not route calls to the PSTN (i.e. an endpoint connected to a different PBX) regardless of the network site to which the Mediation Server peer is associated. All inbound calls, outbound calls, call transfers and call forwards involving PSTN endpoints will be subject to Location Based Routing to use only PSTN gateways that are defined as local to

such Mediation Server peer.

## Scenarios for Location-Based Routing

Location-Based Routing applies the following general rules when routing calls in the following scenarios.

### Outgoing calls

The routing of outbound calls of users enabled for Location-Based Routing is affected by the network location of the user's endpoint. The following table illustrates how Location-Based Routing affects the routing of outbound calls depending on the location of the caller's endpoint.

#### Caller placing an outbound call to the PSTN

	<b>USER ENDPOINT LOCATED IN A NETWORK SITE ENABLED FOR LOCATION-BASED ROUTING</b>	<b>USER ENDPOINT LOCATED IN UNKNOWN NETWORK SITE OR NOT ENABLED FOR LOCATION-BASED ROUTING</b>
Authorization of outbound calls	Call is authorized based on user's voice policy	Call is authorized based on user's voice policy
Routing of outbound call	Call is routed according to the network site's voice routing policy	Call is routed according to user's voice policy and only through trunks not enabled for Location-Based Routing (if available)

### Incoming Calls

The routing of incoming calls to users enabled for Location-Based Routing depends on the location of the user's endpoint. The routing of incoming calls is affected in the following way. If a user has an incoming call to an endpoint located in a Location-Based Routing enabled network site, and the endpoint is located in the same network site as the PSTN gateway, the call will be routed. If a user has an incoming call to an endpoint located in a Location-Based Routing enabled network site, and the endpoint is located in a different network site than the PSTN gateway, the call will not be routed. When a user has no endpoints located in the same network site as the PSTN gateway where the incoming call is originating from, the incoming call will be routed directly to the user's voicemail and a missed call notification will be sent to the called party.

The call forwarding settings of a user that is enabled for Location-Based Routing will continue to be enforced, however, calls forwarded will be subject to Location-Based Routing restrictions of the user.

The following table illustrates how Location-Based Routing affects the routing of inbound calls depending on the location of the callee's endpoint. The network site of the PSTN gateway is enabled for Location-Based Routing, and Location-Based Routing only permits routing of PSTN calls to endpoints within the same network site.

#### Callee receiving an inbound call from the PSTN

	<b>CALLEE'S ENDPOINT LOCATED IN THE SAME NETWORK SITE AS PSTN GATEWAY</b>	<b>CALLEE'S ENDPOINT NOT LOCATED IN THE SAME NETWORK SITE AS PSTN GATEWAY</b>	<b>CALLEE'S ENDPOINT LOCATED IN UNKNOWN NETWORK SITE OR NOT ENABLED FOR LOCATION-BASED ROUTING</b>
Routing of inbound PSTN call	Incoming call is routed to callee's endpoints	Incoming call is not routed to callee's endpoints	Incoming call is not routed to callee's endpoints

### Call transfers and call forwarding

When a PSTN endpoint is involved, Location-Based Routing analyzes the location of the callee's endpoint and the endpoint where the call will be transferred or forwarded to (i.e. transfer/forward target). Location-Based Routing determines whether the call should be transferred or forwarded depending on the location of both endpoints.

The following table illustrates the scenario of a Skype for Business user in a call with a PSTN endpoint, and the Skype for Business user transfers the call to another Skype for Business user. Depending on the network site location of the transferee's endpoint, Location-Based Routing affects the routing of the call transfer or forward.

### Initiating call transfer or forward

USER INITIATING THE CALL TRANSFER/FORWARD	TARGET ENDPOINT IS IN SAME NETWORK SITE AS USER INITIATING CALL TRANSFER OR FORWARD	TARGET ENDPOINT IS IN DIFFERENT NETWORK SITE AS USER INITIATING CALL TRANSFER OR FORWARD	TARGET ENDPOINT IS IN UNKNOWN NETWORK SITE OR NETWORK SITE NOT ENABLED FOR LOCATION-BASED ROUTING
Skype for Business user	Call forward or transfer is allowed	Call forward or transfer is not allowed	Call forward or transfer is not allowed

For example: a Skype for Business user in a call with a PSTN endpoint transfers the call to another Skype for Business user that is in the same network site. In this case, the call transfer is allowed.

The following table illustrates the scenario of a Skype for Business user in a call with another Skype for Business user, and one of the users transfers the call to a PSTN endpoint. Depending on the location of the user the call is being transferred to, the table details how Location-Based Routing affects the call.

### Call transfer or forward to PSTN endpoint

CALL TRANSFER/FORWARD ENDPOINT TARGET	SKYPE FOR BUSINESS USERS IN SAME NETWORK SITE	SKYPE FOR BUSINESS USERS IN DIFFERENT NETWORK SITES	ONE OR BOTH SKYPE FOR BUSINESS USERS IN UNKNOWN NETWORK SITE OR NETWORK SITE NOT ENABLED FOR LOCATION-BASED ROUTING
PSTN endpoint	Call forward or transfer allowed by the transferred user's site voice routing policy	Call forward or transfer allowed by the transferred user's site voice routing policy	Call forward or transfer allowed by the transferred user's voice policy only through trunks not enabled for Location-Based Routing

For example: a Skype for Business user in a call with another Skype for Business user that is in the same network site transfers the call to a PSTN endpoint and the call transfer is allowed.

### Simultaneous ringing

When the called party has simultaneous ringing enabled, Location-Based Routing analyzes the location of the calling party and the endpoints of the called parties to determine whether the call should be routed.

The following table illustrates a user configured with simultaneous ringing, and the simultaneous ringing target is a user in the same network site, in a different network site, or in an unknown network site.

INCOMING PSTN CALL FOR	LOCATED IN THE SAME NETWORK SITE AS CALLEE	LOCATED IN DIFFERENT NETWORK SITE THAN CALLEE	LOCATED IN UNKNOWN NETWORK SITE OR NOT ENABLED FOR LOCATION-BASED ROUTING
Skype for Business user	Simultaneous ring allowed	Simultaneous ring not allowed	Simultaneous ring not allowed

The following table illustrates a call from a Skype for Business user (i.e. Skype for Business caller) in the same network site, in a different network site, or from an unknown network site. The callee has a PSTN endpoint (i.e. cellphone) configured as a simultaneous ring target. In this scenario, Location-Based Routing will determine whether the call should be routed to the simultaneous ring target (i.e. cellphone) of the callee or not.



<b>SIMULTANEOUS RING TARGET</b>	<b>LOCATED IN THE SAME NETWORK SITE AS CALLEE</b>	<b>LOCATED IN DIFFERENT NETWORK SITE THAN CALLEE</b>	<b>LOCATED IN UNKNOWN NETWORK SITE OR NOT ENABLED FOR LOCATION-BASED ROUTING</b>
PSTN endpoint	Simultaneous ring allowed through the caller's site voice routing policy	Simultaneous ring allowed through the caller's site voice routing policy	Simultaneous ring allowed through the caller's voice policy to trunks not enabled for Location-Based Routing

### Skype for Business Cumulative Update 4

With Cumulative Update 4, you're going to see the following:

- Location-Based Routing will continue to be enabled via Voice Policy, including Skype for Business Mobile clients.
- The calling behavior for Skype for Business Mobile clients will be based on whether they're enabled for Location-Based Routing, and the communicating client. This is designed to be static, but there may be, in certain situations, an effort to associate a Skype for Business Mobile client to a local PSTN gateway, and allow certain behaviors, such as an escalation
- Regardless of your OS, your Skype for Business Mobile client should have the same functionality.

The following table will walk you through some of the post-Cumulative Update 4 scenarios:

<b>LOCATION-BASED ROUTING USER</b>	<b>OTHER PARTY</b>	<b>ACTION</b>	<b>RESULT</b>
Skype for Business Mobile	PSTN	Skype for Business Mobile receives an incoming PSTN call.	The call is routed via Call via Work (CvW), and not VoIP.
Skype for Business Mobile	PSTN	Skype for Business Mobile makes an outgoing PSTN call.	The call is routed via CvW, and not VoIP.
Skype for Business Mobile	PSTN	Skype for Business Mobile is in a PSTN call. Skype for Business Mobile then escalates the call to another user or contact.	The call is routed via VoIP if the user or contact is local to the PSTN gateway leg. If the user or contact is remote from the PSTN gateway leg, the call is routed via CvW. If the target user is not reachable via the PSTN, then the call fails. If the target contact is a Conference Auto Attendant (CAA), the call is blocked.
Skype for Business Mobile	Skype for Business client or Federated user	A Skype for Business Mobile initiates a voice call to another Skype for Business client or Federated user.	The call is completed via VoIP.
Skype for Business Mobile	Skype for Business client or Federated user	A Skype for Business client or Federated user initiates a voice call to a Skype for Business Mobile Location-Based Routing user.	The call is completed via VoIP.

LOCATION-BASED ROUTING USER	OTHER PARTY	ACTION	RESULT
Skype for Business Mobile	Skype for Business client or Federated user	A Skype for Business client or Federated user is on a VoIP call to a Skype for Business Mobile user. Either party escalates to an additional Skype for Business or Federated user.	The call is completed via VoIP.
Skype for Business Mobile	Federated User	A Federated User is on voice call to a Skype for Business Mobile Location-Based Routing user; a Skype for Business Mobile party escalates to a PSTN user.	The call is blocked.
Skype for Business Mobile	Federated User	A Federated user is on a VoIP call to a Skype for Business Mobile Location-Based Routing user; either party escalates to a CAA contact.	The escalated call is blocked, with an appropriate error message.
Skype for Business Mobile	Federated User	A Federated user is on a VoIP call to a Skype for Business Mobile Location-Based Routing user, and the Federated user escalates to a PSTN user.	The escalation will be allowed or disallowed based on the Location-Based Routing of the Federated user. The Skype for Business Mobile Location-Based Routing user's application doesn't take any action.

## Delegation

The delegation capabilities in Skype for Business are affected by Location-Based Routing in the following manner:

- When a delegate enabled for Location-Based Routing places a call on behalf of a manager, the delegate's voice policy is used to authorize the call and the delegate's site voice routing policy will be used to route the call
- For incoming PSTN calls to a manager, the same rules applicable for call forwarding or simultaneously ringing will apply as described in the Call transfers and forwarding and Simultaneous ringing topics.
- When a delegate sets a PSTN endpoint as a simultaneous ring target, for an incoming call to the manager, the voice routing policy of the site that is associated to the incoming trunk will be used to route the call to the delegate's PSTN endpoint.
- For delegation, it's recommended that the manager and his associated delegates to be usually located in the same network site.

## Other planning considerations

When planning Location-Based Routing, you should consider the impact to the following scenarios.

### Disaster Recovery

During a failover from the primary pool to a backup pool as well as when restoring normal operations to the primary pool, Location-Based Routing remains enforced at all times during a disaster and recovery procedure.

## Survivable Branch Appliance

Configuring Location-Based Routing impacts the planning of where you deploy the gateways associated to your Survivable Branch Appliances. The gateway associated to your SBA must be located in the same network site as your Survivable Branch Appliance; otherwise, users homed on your Survivable Branch Appliance will not be permitted to place outbound calls if Location-Based Routing is configured. When the WAN connection between your Survivable Branch Appliance and the central site is down, Location-Based Routing restrictions remains enforced.

## Client and server support for Location-Based Routing

Location-Based Routing is enforced by Skype for Business Server. Skype for Business Server can identify the network sites where users are connecting from within the corporate network. Since remote users are outside the corporate network, their location is considered to be unknown.

### Server Support

Location-Based Routing requires that Skype for Business Server or Lync Server 2013 CU1 is deployed on all Front End pools and Standard Edition servers in a given topology. If these versions of the server are not installed, Location-Based Routing restrictions cannot be fully enforced.

The following table identifies the combination of server roles and versions that is supported for Location-Based Routing.

POOL VERSION	MEDIATION SERVER VERSION	SUPPORTED
Skype for Business Server or Lync Server 2013 February 2013 Cumulative Update	Skype for Business Server or Lync Server 2013 February 2013 Cumulative Update	yes
Skype for Business Server or Lync Server 2013 February 2013 Cumulative Update	Lync Server 2013	no
Skype for Business Server or Lync Server 2013 February 2013 Cumulative Update	Lync Server 2010	no
Skype for Business Server or Lync Server 2013 February 2013 Cumulative Update	Office Communications Server 2007 R2	no
Lync Server 2013	any	no
Lync Server 2010	any	no
Office Communications Server 2007 R2	any	no

### Client Support

The following table identifies the clients that Location-Based Routing supports.

CLIENT TYPE	SUPPORTED	DETAILS
Skype for Business	yes	

CLIENT TYPE	SUPPORTED	DETAILS
Lync 2013	yes	
Lync 2010	yes	
Office Communicator 2007 R2	no	
Lync Phone Edition	yes	
Lync Attendant	yes	
Lync for Windows 8	no	
Lync Mobile 2013	no	VoIP must be disabled for Lync Mobile 2013 clients if used by users with Location-Based Routing enabled.
Lync Mobile 2010	yes	

#### NOTE

To disable VoIP for Skype for Business clients, assign a mobility policy with the setting, IP Audio/Video, disabled for all users enabled for Location-Based Routing. For more details about mobility policy, see [New-CsMobilityPolicy](#).

## Capabilities not supported by Location-Based Routing

Location-Based Routing does not apply to the following types of interactions. Location-Based Routing is not enforced when Skype for Business endpoints interact with PSTN endpoints using these capabilities.

- PSTN dial-in to conferences
- Incoming and outgoing PSTN calls through Response Group
- Call park or retrieval of PSTN calls through Call Park
- Incoming PSTN calls to Announcement Service
- Incoming PSTN calls retrieved via Group Call Pickup

To enforce Location-Based Routing rules to the types of interactions in the following list, you must enable Location-Based Routing for Conferencing:

- PSTN dial-out from conferences
- Escalations from peer-to-peer audio conversations to conferencing involving PSTN endpoints
- Consultative transfers involving PSTN endpoints

To enable Location-Based Routing for Conferencing, see [Location-Based Routing for Conferencing](#).

# Location-Based Routing for Conferencing in Skype for Business Server

5/20/2019 • 11 minutes to read

Planning for location-based routing for conferencing in Skype for Business Server Enterprise Voice, including consultative call transfers.

Location-Based Routing makes it possible to restrict the routing of calls between VoIP endpoints and PSTN endpoints based on the location of the parties in the call. Location-Based Routing for Conferencing enables you to enforce Location-Based Routing rules on meetings (i.e. conferences) to prevent PSTN toll bypass. The application monitors an active conference and enforces Location-Based Routing restrictions based on the location of users participating. The Location-Based Routing for Conferencing application additionally enables the enforcement of Location-Based Routing restrictions to consultative transfers involving PSTN endpoints.

The Location-Based Routing Conferencing application provides to Skype for Business Conferences a mechanism for the prevention of PSTN toll bypass. The application monitors active conferences and enforces Location-Based Routing restrictions based on the location of the Skype for Business users participating.

The Location-Based Routing Conferencing application determines whether Location-Based Routing is to be enforced on a Skype for Business meeting if the following criteria are met:

- The meeting organizer is enabled for Location-Based Routing. Location-Based Routing restrictions will be applied only to conferences that are organized by users who are enabled for Location-Based Routing.
- At least one meeting participant is a PSTN endpoint. Location-Based Routing restrictions are applicable only for conferences that include PSTN endpoints.
- The network site where the PSTN gateway used to bridge the conference to the PSTN is located as well as the network sites where the organizers and participants are connecting from.

The Location-Based Routing for Conferencing application prevents the participation of Skype for Business users and PSTN endpoints from different network sites to the same conference. If the organizer of a meeting is enabled for Location-Based Routing, the Conferencing application enforces the following restrictions:

- The endpoints that can join a Skype for Business meeting depend on the endpoints that already joined the conference, and this restriction adjusts as joined endpoints leave and new endpoints join the conference. If organizers and participants are joining a Skype for Business meeting from the same network site, then a PSTN endpoint, another participant from the same network site, another participant from a different network site or a participant from an unknown network site are allowed to join.
- If organizers and participants are joining the meeting from different or unknown network sites, a PSTN endpoint is not allowed to join the meeting if the PSTN call ingresses from a SIP trunk enabled for Location-Based Routing.
- If organizers and participants are all joining the meeting from the same network site and there are participants joining the same meeting from the PSTN, a Skype for Business endpoint from a different network site is not allowed to join the meeting.

These conferencing Location-Based Routing restrictions are summarized in the following table.

||

USER(S) IN A CONFERENCE AT ANY GIVEN POINT	USER(S) ALLOWED TO JOIN THE CONFERENCE	USER(S) NOT ALLOWED TO JOIN THE CONFERENCE
Skype for Business VoIP client user(s) from a single network site	Skype for Business VoIP client user from the same network site Skype for Business VoIP client user from a different network site Skype for Business VoIP client user from an unknown network site Federated Skype for Business VoIP client user User joining from a PSTN endpoint	None
Skype for Business VoIP client user(s) from an unknown network site	Skype for Business VoIP client user from any site Skype for Business VoIP client user from an unknown site Federated Skype for Business VoIP client user	User joining via a PSTN endpoint
Skype for Business VoIP client users from different network sites	Skype for Business VoIP client user from any network site Skype for Business VoIP client user from an unknown network site Federated Skype for Business VoIP client user	User joining via a PSTN endpoint
Skype for Business VoIP client user(s) from a single network site and users joining from a PSTN endpoint	Skype for Business VoIP client user from the same network site	Skype for Business VoIP client user from a different network site Skype for Business VoIP client user from an unknown network site Federated Skype for Business VoIP client user

The following are additional characteristics of the Location-Based Routing for Conferencing application:

- When a user is not allowed to join a conference given Location-Based Routing restrictions, the call to the conference will be rejected and the Skype for Business client will report that the call was not completed or has ended.
- A PSTN endpoint joining a conference with Location-Based Routing enforcements will not be restricted to join the conference regardless of its state if the endpoint joins via a trunk that is not enabled for Location-Based Routing.
- A PBX system connected to a Mediation Server over a SIP trunk that does not egress calls to the PSTN will have the same enforcements as Skype for Business users located in the same network site where the SIP trunk is defined. For example, a PSTN endpoint will be able to join a conference with a PBX user and a Skype for Business user if they are located in the same network site; otherwise, the PSTN endpoint will not be allowed to join the conference if the PBX user is in a different network site than the Skype for Business user.

**NOTE**

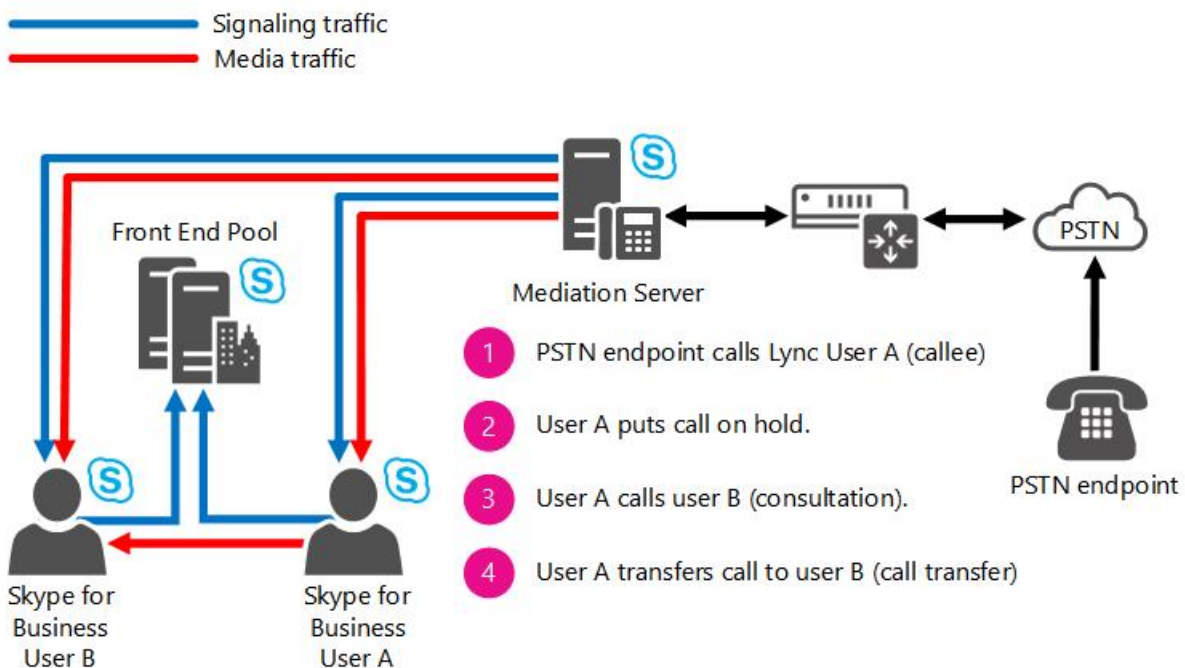
With Skype for Business Cumulative Update 4, the behavior in the following table should be observed:

USER	OTHER PARTY	ACTION	RESULT
Skype for Business Mobile	PSTN	Skype for Business Mobile is in a PSTN call. Skype for Business Mobile then escalates the call to a Conference Auto Attendant (CAA).	The call is blocked, with an appropriate error message.
Skype for Business Mobile	Skype for Business Client or Federated User	The Client or Federated User is on a VoIP call to a Skype for Business Mobile Location-Based Routing user, and either party escalates to a CAA.	The escalation call is blocked, with an appropriate error message.

## Consultative call transfers

In addition to enforcing Location-Based Routing to Skype for Business meetings, the Location-Based Routing for Conferencing application enforces Location-Based Routing restrictions on consultative call transfers that egress to PSTN endpoints. A consultative call transfer is a call established between two parties where one of the parties transfers the call to a new user. For example, a PSTN endpoint calls user A (Skype for Business callee). User A determines the PSTN user should be forwarded to user B (Skype for Business user). User A places the call with the PSTN user on hold, and calls user B. User B agrees to talk to the PSTN user. User A transfers the call on-hold to user B.

### Consultative call transfer call flow



When a user enabled for Location-Based Routing initiates a consultative call transfer of a PSTN endpoint (as shown in the preceding figure), this creates two active calls, one call between the PSTN user and Skype for Business user A, and the other between Skype for Business user A and Skype for Business user B. the following behavior is enforced by the Location-Based Routing for Conferencing application:

- If the SIP trunk routing the PSTN call is authorized to re-route the PSTN call to the network site where Skype for Business user B (i.e. transfer target) is located,, then the call transfer will be allowed; otherwise, the consultative call transfer will be blocked. This authorization is performed based on the transferred party's location being in the same network site as the SIP trunk that is routing the active call to the PSTN endpoint.

- If the SIP trunk routing the inbound PSTN call is not authorized to route calls to the network site where the transferred party (Skype for Business user B) is located or the transferred party is located in an unknown network site, then the consultative call transfer to the PSTN endpoint (i.e. call transfer target) will be blocked.

The following table describes how Location-Based Routing restrictions are applied by the Location-Based Routing for Conferencing application for consultative call transfers. Although PBX endpoints are not directly associated with a network site, the SIP trunk the PBX is connected to can be assigned a network site. Therefore, the PBX endpoint can be indirectly associated with a network site.

<b>NETWORK SITE OF CALL TRANSFERRED PARTY</b>	<b>NETWORK SITE OF CALL TRANSFER TARGET</b>	<b>BEHAVIOR</b>
PSTN endpoint	Skype for Business user in the same network site (i.e. site 1)	Consultative transfer will be allowed
PSTN endpoint	Skype for Business user in different network sites (i.e. site 2)	Consultative transfer will be disallowed
PSTN endpoint	Skype for Business user in an unknown network site	Consultative transfer will be disallowed
PSTN endpoint	Federated Skype for Business user	Consultative transfer will be disallowed
PSTN endpoint	PBX endpoint in the same site (i.e. site 1)	Consultative transfer will be allowed
PSTN endpoint	PBX endpoint in a different sites (i.e. site 2)	Consultative transfer will be disallowed
PBX endpoint in the same site (i.e. site 1)	PSTN endpoint	Consultative transfer will be allowed
PBX endpoint in a different site (i.e. site 2)	PSTN endpoint	Consultative transfer will be disallowed
PBX endpoint in any site	Skype for Business user in the same network site (i.e. site 1)	Consultative transfer will be allowed
PBX endpoint in any site	Skype for Business user in different network sites (i.e. site 2)	Consultative transfer will be allowed
PBX endpoint in any site	Skype for Business user in an unknown network site	Consultative transfer will be allowed
PBX endpoint in any site	Federated Skype for Business user	Consultative transfer will be allowed

## Requirements

The Location-Based Routing for Conferencing application requires that either Skype for Business Server or Lync Server 2013 Cumulative Update 2 is deployed on all Front-End pools and Standard Edition Servers in your topology. If these server versions are not installed on some servers in your topology, Location-Based Routing restrictions cannot be fully enforced on meetings and consultative call transfers.

The following table identifies the combination of server roles and versions that support Location-Based Routing.



FRONT-END POOL VERSION	MEDIATION SERVER VERSION	SUPPORTED
Skype for Business Server or Lync Server 2013 Cumulative Update 2	Skype for Business Server or Lync Server 2013 Cumulative Update 2	Yes
Lync Server 2013 Cumulative Update 2	Lync Server 2013 Cumulative Update 1	No
Lync Server 2013 Cumulative Update 2	Lync Server 2010	No
Lync Server 2013 Cumulative Update 2	Office Communications Server 2007 R2	No
Lync Server 2013 Cumulative Update 1	Any	No
Lync Server 2010	Any	No
Office Communications Server 2007 R2	Any	No

## Configuration of Location-Based Routing for Conferencing

The Location-Based Routing for Conferencing application relies on the configuration of Location-Based Routing. The main configurations are the following:

- The location of participants joining a meeting is determined based on their network site. A network site and its associated network subnets must be defined in Skype for Business Server in order to enforce Location-Based Routing.
- To enforce Location-Based Routing of meetings, Skype for Business participants must be enabled for Location-Based Routing.
- To enforce Location-Based Routing of PSTN endpoints joining meetings, the SIP trunk used to connect the PSTN endpoints must be configured for Location-Based Routing.

## Enabling the Location-Based Routing for Conferencing

The Location-Based Routing for Conferencing application is disabled by default. Before enabling this application, you need to determine the right priority to assign for the application. To determine this priority, run the following cmdlet in Skype for Business Server Management Shell:

`Get-CsServerApplication -Identity Service:Registrar`: In this cmdlet, <Pool FQDN> is the pool in which the Location-Based Routing for Conferencing application is to be enabled.

This cmdlet will return the list of the applications hosted by Skype for Business Server and the priority value for each of them. The Location-Based Routing for Conferencing application needs to be assigned a priority value larger than the "UdcAgent" application and smaller than the "DefaultRouting", "ExumRouting" and "OutboundRouting" applications. We recommend that you assign the Location-Based Routing for Conferencing application a priority value that is one point higher than the priority value of the "UdcAgent" application.

For example, if the "UdcAgent" application has a priority value of "2", the "DefaultRouting" application has a priority value of "8", the "ExumRouting" application has a priority value of "9" and the "OutboundRouting" application has a priority value of "10" then you should assign the Location-Based Routing for Conferencing application a priority value of "3". Doing so would place the priority of the applications in the following order: Other applications (Priorities: 0 to 1), "UdcAgent" (Priority: 2), Location-Based Routing Conferencing application (Priority: 3), other applications (Priorities: 4 to 8), "DefaultRouting" (Priority: 9), "ExumRouting" (Priority: 10) and "OutboundRouting" (Priority: 11).

After you find the correct priority value for the Location-Based Routing for Conferencing application, type the following cmdlet for each Front-End pool or Standard Edition Server that homes users enabled for Location-Based Routing:

```
New-CsServerApplication -Identity Service:Registrar:<Pool FQDN >/LBRouting -Priority <Application Priority> - Enabled $true -Critical $true -Uri http://www.microsoft.com/LCS/LBRouting
```

For example:

```
New-CsServerApplication -Identity Service:Registrar:LS2013CU2LBRPool.contoso.com/LBRouting -Priority 3 - Enabled $true -Critical $true -Uri http://www.microsoft.com/LCS/LBRouting
```

After using this cmdlet, restart all Front End servers in the pool or the Standard Edition Servers where the Location-Based Routing for Conferencing application has been enabled.

#### **IMPORTANT**

Location-Based Routing enforcements to conferences or consultative transfers won't be enforced until all the Front End Servers in the applicable pools or the Standard Edition Servers are restarted. If you set **-Critical to \$true** in the preceding cmdlets, your Skype for Business Server services will be immediately restarted. If you do not want these services to immediately restart, set **-Critical to \$false** for now, and then use **Set-CsServerApplication** to change **-Critical to \$true** later, after the services have been restarted.

Once the Location-Based Routing for Conferencing application has been successfully enabled and all applicable servers have been restarted, all conferences organized by Skype for Business users enabled for Location-Based Routing will be monitored to prevent PSTN toll bypass

# Plan for call management features in Skype for Business

5/20/2019 • 2 minutes to read

Overview of supported call-management features in Skype for Business Server Enterprise Voice.

Enterprise Voice call management features control how incoming calls are routed and answered. Skype for Business Server provides the following call management features:

- **Call Park:** Enables voice users to temporarily park a call and then pick it up from the same or another phone.
- **Group Pickup:** Enables voice users to pick up calls that are ringing for other voice users who are assigned to call pickup groups.
- **Response Group:** Routes incoming calls to groups of agents by using hunt groups or interactive voice response (IVR) questions and answers.
- **Announcement:** Plays a message for calls made to an unassigned number, or routes the call elsewhere, or both.

If you plan to deploy Enterprise Voice, you can choose to implement any or all of these call management features.

## In this section

- [Planning for Call Parking](#)
- [Planning for Group Pickup](#)
- [Planning for Response Groups](#)
- [Planning for Announcements](#)

# Plan for Call Park in Skype for Business

5/20/2019 • 5 minutes to read

Planning for call park in Skype for Business Server Enterprise Voice, which enables putting calls on hold and transferring calls to departments. Includes capacity planning, supported calls, and supported clients.

The Call Park application enables Enterprise Voice users to do the following:

- Put a call on hold and then retrieve the call from the same phone or another phone.
- Put a call on hold to transfer it to a department or general area (for example, to a sales department or a warehouse where there is a common area phone).
- Put a call on hold and keep the original answering phone free for other calls.

When a user parks a call, Skype for Business Server transfers the call to a temporary number, called an orbit, where the call is held until it is retrieved or it times out. Skype for Business Server sends the orbit to the user who parked the call. To retrieve the parked call, the user can dial the orbit number or click the orbit link or button in the Conversation window.

The user who parked a call can notify someone to retrieve the call by using an external mechanism, such as instant messaging (IM) or a paging system, to communicate the orbit number to someone else. The user who parked the call can leave the Conversation window open to receive notification when the call is retrieved.

Because orbit ranges are globally unique, it is possible to retrieve calls from any Skype for Business Server site or PBX phone if routing is configured appropriately. If no one retrieves the call within a configurable amount of time, the call rings back to the person who parked it. If that person does not answer the ringback, the call is transferred to a fallback destination, such as to an operator, if so configured. You can configure the number of times the call rings back before being transferred from one to ten times. If no one answers a transferred call, the call is disconnected. The orbit is freed when the call is retrieved or disconnected.

When you deploy Call Park, you need to reserve ranges of extension numbers for parking calls. These extensions need to be virtual extensions: extensions that have no user or phone assigned to them. You then configure the call park orbit table with the ranges of extension numbers and specify which Application service hosts the Call Park application that handles each range. Each Front End pool has a Call Park table on the corresponding Back End Server that is used to manage calls that are parked on the pool. The list of orbit ranges is stored in Central Management store and is used to route orbits to the destination pool. Each Skype for Business Server pool where the Call Park application is deployed and configured can have one or more orbit ranges. Orbit ranges must be globally unique across the Skype for Business Server deployment.

You also configure other Call Park settings, such as where calls are redirected if they time out and whether the person on the phone hears music while parked. You can also specify the music file to play while the call is on hold.

## NOTE

Customized music-on-hold files for Call Park are not backed up as part of the Skype for Business Server disaster recovery process and will be lost if the files uploaded to the pool are damaged, corrupted, or erased. Always keep a separate backup copy of the customized music-on-hold files that you have uploaded for Call Park.

The Call Park application is a component of Enterprise Voice. When you deploy Enterprise Voice, the Call Park application is installed and activated automatically. Before you can use Call Park, however, the Enterprise Voice administrator must configure it and enable it for users through voice policy.

# Deployment and requirements

The Call Park application is automatically installed when you deploy Enterprise Voice. You enable Call Park by configuring voice policy.

## Software requirements

All Front End Servers and Standard Edition servers where Call Park is deployed must have the Windows Media Format Runtime installed for servers running Windows Server 2008 R2, or Microsoft Media Foundation for servers running Windows Server 2012 or Windows Server 2012 R2. For Windows Server 2008 R2, Windows Media Format Runtime is installed as part of Windows Desktop Experience. Windows Media Format Runtime or Microsoft Media Foundation is required for Windows Media Audio (.wma) files that Call Park plays for music on hold.

## Port requirements

The Call Park application uses **Port 5075** for SIP listening requests.

### NOTE

This port is a default setting that you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Lync Server Management Shell documentation.

## Audio File requirements

The Call Park application supports only Windows Media Audio (.wma) files for music on hold. You can use the Microsoft Expression Encoder 4 to customize files for music on hold. To download Expression Encoder 4, see "[Expression Encoder 4](#)". Use the tool to convert the file to a .wma format. The recommended format for Call Park music-on-hold files is Media Audio 9, 44 kHz, 16 bits, Mono, CBR, 32 kbps.

### NOTE

The converted file plays over the phone only at 16 kHz, even if it was recorded at 44 kHz.

# Supported clients and calls

The following clients and types of calls are supported for Call Park

## Clients Supported for Parking Calls

Calls from any IP, private branch exchange (PBX), public switched telephone network (PSTN), or mobile phone can be parked.

### NOTE

Only audio calls can be parked. Instant messages and conferences cannot be parked.

The following clients can use Call Park to park calls:

- Skype for Business
- Lync 2013
- Lync 2010
- Lync 2010 Attendant
- Lync Phone Edition

**NOTE**

Mobile phones cannot use Call Park to park calls.

**Clients Supported for Retrieving Calls**

Orbit ranges are configured as blocks of virtual extensions (extensions without an assigned user or phone). When you configure orbits as virtual extensions, mobile phones and PSTN phones cannot retrieve parked calls.

Federated users cannot retrieve parked calls.

The following clients can retrieve calls that are parked on Call Park:

- Skype for Business
- Lync 2013
- Lync 2010
- Lync 2010 Attendant
- Lync Phone Edition
- IP common area phones
- Non-IP phones that are connected to the Skype for Business Server infrastructure, including common area phones and private branch exchange (PBX) phones

## Call Park capacity planning

The following table describes the Call Park user model that you can use as the basis for capacity planning requirements.

**IMPORTANT**

Keep in mind that, for disaster recovery capacity planning, each pool of a paired pool should be able to handle the workloads for Call Park services in both pools.

**Call Park User Model**

<b>METRIC</b>	<b>PER FRONT END POOL (WITH 8 FRONT END SERVERS)</b>	<b>PER STANDARD EDITION SERVER</b>
Park rate	8 per minute	1 per minute
Retrieve parked call rate	8 per minute	1 per minute
Average park duration	60 seconds	60 seconds

# Plan for Group Call Pickup in Skype for Business

5/20/2019 • 7 minutes to read

Planning for Group Call Pickup in Skype for Business Server Enterprise Voice, which enables users to answer calls originally intended for others.

Group Call Pickup enables users to answer incoming calls to their colleagues from their own phones. This increases the availability of a user's line by enabling other users to answer an incoming call by dialing a call pickup group number. When Group Call Pickup is deployed, the number of incoming calls that are routed to voice mail can be significantly reduced, which is particularly useful for calls from customers who are external to your organization.

The Group Call Pickup feature is designed in particular for business units in open office environments. Incoming calls are not disruptive because they ring only at the intended destination. Other users who hear the ring, however, can still pick up the call simply by dialing the group number.

In environments where users are not located in an open office layout, or where users who share a common responsibility are geographically distributed, team call presents the most suitable solution. The primary difference between Group Call Pickup and team call is that, with Group Call Pickup, an incoming call rings only at the intended destination, but anyone can still choose to answer it by dialing a group number. With team call, the call rings at all the team members' phones, and any user in the team can pick up the phone to answer the call. An additional difference between Group Call Pickup and team call is that Group Call Pickup is managed by an administrator, through Skype for Business Server. With team call, end users manage the feature by using the Skype for Business client. With Group Call Pickup, therefore, this aspect of call management can be centralized.

Group Call Pickup is built on the Call Park application. When you deploy Group Call Pickup, you configure the call park orbit table with separate ranges of extension numbers that are designated as call pickup group numbers. Like call park orbit numbers, call pickup group numbers must be virtual extensions that have no user or phone assigned to them. Each Front End pool where you deploy Group Call Pickup can have one or more ranges of call pickup group numbers. The group number ranges must be globally unique across the Skype for Business Server deployment.

## NOTE

Number ranges that are designated as Group Call Pickup numbers in the call park orbit table cannot be managed or viewed by using the Skype for Business Server Control Panel. The only way to see all the number ranges in the call park orbit table is to use Skype for Business Server Management Shell. Similarly, the only way to add, modify, or remove Group Call Pickup numbers is to use Skype for Business Server Management Shell.

After you configure the call pickup group numbers, you assign users to a call pickup group. Any user who is assigned to a call pickup group can have their calls answered by other users. When a call comes in to a user who is assigned to a call pickup group, any other user who notices the call can answer it by manually dialing the call pickup group number. The user who picks up the call does not need to be a member of the group. When a call is picked up by another user, a notification is sent to the number originally called.

## NOTE

A user can be a member of only one call pickup group.

#### NOTE

Although any user in the Skype for Business Server deployment can answer a call to a call pickup group member, the person answering the call must know the correct call pickup group number to dial.

If a user dials a call pickup group number to answer a call when multiple phones in the group are ringing, the user answers the call that has been ringing the longest.

Simultaneous ringing settings will work for users who have group call pickup. That is, a call made to a user who has Group Call Pickup will ring for all the configured destinations, and another user can answer the call. The exception to this rule is when the user configures simultaneous ringing to call all the team members.

Group Call Pickup cannot be used to answer the following types of calls:

- Calls to a private line
- Calls from a contact who has been assigned the Friends and Family privacy relationship

#### TIP

A user who is a member of a call pickup group can prevent certain calls from being retrieved through Group Call Pickup by marking the contact as a personal contact in the Skype for Business client. To mark a contact as a personal contact, set the Privacy Relationship for the contact to Friends and Family. Any incoming call from contacts with the Privacy Relationship set to Friends and Family cannot be retrieved by using Group Call Pickup.

- Video portion of audio/video calls

#### NOTE

If a user answers an audio/video call, the user receives only the audio. Either the person calling or the person answering the call can escalate the call to add video.

- Simultaneous ringing calls that are routed to team call members
- Calls routed to a delegate
- Calls routed to a response group

The following types of users cannot participate in Group Call Pickup. That is, they should not be included in a Group Call Pickup group, and they cannot pick up calls for users who have Group Call Pickup enabled.

- Users who are homed online in a hybrid deployment
- Users who are not homed on either a Skype for Business Server 2015 pool or a Lync Server 2013 pool with Cumulative Updates for Lync Server 2013: February 2013 in an on-premises deployment

If no one answers a call to a member of a call pickup group, the call is routed as specified in the client settings. That is, the call goes to voicemail or is forwarded to a different destination, as specified in the client settings.

## Deployment and requirements

Group Call Pickup is automatically deployed when you deploy Enterprise Voice and the Call Park application. You enable Group Call Pickup by configuring the Call Park orbit table with separate ranges of numbers designated as call pickup group numbers, and then by assigning users to call pickup groups and enabling the users for Group Call Pickup.



# Clients supported for Group Call Pickup

Any of the following clients can be used to answer calls to Group Call Pickup members:

- Skype for Business
- Lync 2013
- Lync 2010
- Lync Phone Edition

## NOTE

Users can use any of these clients to answer calls to Group Call Pickup members, but the users must be homed on a Skype for Business Server pool or a Lync Server 2013 pool with Cumulative Updates for Lync Server 2013: February 2013.

The following clients and devices are not supported for picking up calls to Group Call Pickup members:

- Lync Mobile
- Lync app for Windows 8 and Windows RT
- Lync for iPad
- Analog phones
- Phones with public switched telephone network (PSTN) numbers

## Capacity planning

The following table describes the Group Call Pickup user model that you can use as the basis for capacity planning requirements.

## IMPORTANT

Group Call Pickup is based on the Call Park application. Keep in mind that, for disaster recovery capacity planning, each pool of a paired pool should be able to handle the workloads for Call Park services, including Group Call Pickup, in both pools.

### Group Call Pickup User Model

METRIC	PER FRONT END POOL (WITH 8 FRONT END SERVERS)	PER STANDARD EDITION SERVER
Recommended number of users per group	50	50
Recommended number of groups	500	60
Maximum number of users per pool enabled for Group Call Pickup	25,000	3,000
Maximum rate of incoming calls to total users enabled for Group Call Pickup per pool per minute	500	60

<b>METRIC</b>	<b>PER FRONT END POOL (WITH 8 FRONT END SERVERS)</b>	<b>PER STANDARD EDITION SERVER</b>
Maximum rate of calls retrieved by users with Group Call Pickup per pool per minute	200	25

**NOTE**

For Front End pools that have fewer than eight Front End Servers, calculate the metrics linearly. For example, if your Front End pool has one Front End Server, calculate the maximum load as 1/8 of the values shown in the table.

**NOTE**

You can increase or decrease the recommended number of users per group and number of groups as long as you do not exceed the maximum number of users per pool. For example, your Standard Edition server can have 120 groups with 25 users per group because the number of users enabled for Group Call Pickup is still within the user model maximum (that is, 120 groups times 25 users is 3,000 users enabled for Group Call Pickup).

# Plan for the Response Group application in Skype for Business Server

5/20/2019 • 10 minutes to read

Planning for response groups in Skype for Business Server Enterprise Voice, which enables you to set up call routing to groups of users. Includes audio file requirements.

If your organization has groups of people who answer and manage certain types of calls, such as for customer service, an internal help desk, or general telephone support for a department, you can deploy the Response Group application to manage these types of calls. The Response Group application routes and queues incoming calls to designated persons, who are known as agents. You can increase the use of telephone support services and reduce the overhead of running these services by using response groups.

When a caller calls a response group, the call is routed to an agent based on a hunt group or the caller's answers to interactive voice response (IVR) questions. The Response Group application uses standard response group routing methods to route the call to the next available agent. Supported call routing methods include serial, longest-idle, parallel, round robin, and Attendant routing (that is, all agents are called at the same time for every incoming call, regardless of their current presence).

If no agents are available, the call is held in a queue until an agent is available. While in the queue, the caller hears music until an available agent accepts the call. If the queue is full, or if the call times out while in the queue, the caller might hear a message and then is either disconnected or transferred to a different destination, such as a different phone number or voicemail. When an agent accepts the call, the caller might or might not be able to see the agent's identity, depending on how the administrator configures the response group. Agents can either be formal, which means that they must sign in to the group before they can accept calls routed to the group, or informal, which means that they do not sign into and out of the group to accept calls.

## NOTE

Only on-premises users can be agents. If an agent is moved from on-premises to online, Response Group calls will not be routed to that agent.

## NOTE

The Response Group application uses an internal service, called Match Making, to queue calls and find available agents. Each computer that runs the Response Group application runs the Match Making service, but only one Match Making service per pool is active at a time--the others are passive. If the active Match Making service becomes unavailable during an unplanned outage, one of the passive Match Making services becomes active. The Response Group application does its best to make sure that call routing and queuing continues uninterrupted. However, when a Match Making service transition occurs, any calls that are in transfer at the time are lost. For example, if the transition is due to the Front End Server going down, any calls currently being handled by the active Match Making service on that Front End Server are also lost.

## Response group workflows

A workflow defines the behavior of a call from the time that the phone rings to the time that someone answers the call. The workflow specifies the queue to use for holding the call, and specifies the routing method to use for hunt groups or the questions and answers to use for interactive response groups. A workflow also defines settings such as a welcome message, music on hold, business hours, and holidays.

**NOTE**

You must create agent groups and queues before you create a workflow that uses them.

## Management of response groups

In Skype for Business Server, two management roles are available for managing response groups: Response Group Manager and Response Group Administrator. Response Group Administrators can manage any aspect of any response group. Response Group Managers can manage only certain aspects, and only for the response groups that they own. The Manager role can help you reduce your administration costs, because you can delegate limited responsibilities for specific response groups to any user who is enabled for Enterprise Voice. Note that a user can be both a Response Group Manager and a Response Group Administrator.

To accommodate the Manager role, Response Group application uses a **Workflow Type** of Managed or Unmanaged. The following table describes Managed and Unmanaged response groups.

### Managed and Unmanaged Response Groups

RESPONSE GROUP TYPE	DESCRIPTION
Unmanaged	<p>Unmanaged response groups have no assigned Managers. Only the Response Group Administrator can configure these response groups.</p> <p>Multiple unmanaged response groups can share a queue or agent group.</p> <p>When you migrate response groups from a prior version to Skype for Business Server, the type is set to Unmanaged.</p>
Managed	<p>Response Group Administrators can configure any aspect of managed response groups.</p> <p>Response Group Managers cannot view or modify response groups that are not explicitly assigned to them.</p> <p>Response Group Managers can configure only some settings for the response groups that are explicitly assigned to them.</p> <p>Managed response groups can't share any queues or agent groups with any other response group, managed or unmanaged.</p>

The following table describes the actions that Response Group Managers can and cannot perform for the response groups assigned to them.

### Response Group Manager Capabilities

CAN CONFIGURE:	CAN CREATE, DELETE, OR CONFIGURE:	CANNOT:
Agents Welcome message Response Group name Description Display number Business hours Music on hold Status (active/inactive) Hunt group workflows or Interactive voice response (IVR) workflows	Agent Groups Queues Holiday sets	Create or delete any type of workflow Modify core response group settings, such as: <b>SIP URI</b> , <b>Telephone Number</b> , or <b>Workflow Type</b> .

Response Group Managers can use the following tools to manage their designated response groups.

- Skype for Business Server Control Panel

#### NOTE

Response Group Managers can only manage Response Group settings with this tool. Other Skype for Business Server settings are not available to Managers.

- Response Group Configuration Tool
- Skype for Business Server Management Shell

Response Group scales well to departmental or workgroup environments (for details, see [Capacity Planning for Response Group](#)) and can be deployed in entirely new telephony installations. It supports incoming calls from the Enterprise Voice deployment and from the local carrier network. Agents can use Skype for Business, Lync 2013, Lync 2010, Lync 2010 Attendant, or Lync Phone Edition to take the calls routed to them.

## Deployment and requirements

The Response Group application is automatically enabled when you deploy Enterprise Voice.

### Hardware and software requirements

The Response Group application has the same hardware requirements, operating system requirements and software prerequisites as Front End Servers.

If you use Windows Media Audio (.wma) files for Response Group music and announcements, all Front End Servers or Standard Editions servers that run the Response Group application must have the Windows Media Format Runtime installed for servers running Windows Server 2008 R2, or Microsoft Media Foundation for servers running Windows Server 2012 or Windows Server 2012 R2. For Windows Server 2008 R2, Windows Media Format Runtime is installed as part of Windows Desktop Experience.

Response Group uses **Language packs** to support text-to-speech and speech recognition. These speech technologies are used when you configure messages, such as the welcome message and other prompts, and interactive voice response (IVR) questions and answers. By default, the 26 supported language packs are installed when you deploy Skype for Business Server.

### Port Requirements

The Response Group application uses the following ports:

- **Port 5071** for SIP listening requests
- **Port 8404** for interserver communications

#### NOTE

This port is used for the Match Making service and is required when the Response Group application is deployed in a pool that has more than one Front End Server.

#### NOTE

These ports are default settings that you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Skype for Business Server Management Shell documentation.

### Audio File Requirements

The Response Group application supports wave (.wav) file format and Windows Media audio (.wma) file format for

Response Group messages, on-hold music, or interactive voice response (IVR) questions.

The Windows Media audio file format requires that the Windows Media Format Runtime is installed on Front End Servers running Windows Server 2008 R2 and Windows Server 2008. For more details, see "Software Requirements" earlier in this section.

#### Supported Wave File Formats

All wave files must meet the following requirements:

- 8-bit or 16-bit file
- Linear pulse code modulation (LPCM), A-Law, or mu-Law format
- Mono or stereo
- 4MB or less

For the best performance of wave files, a 16 kHz, mono, 16-bit Wave file is recommended.

#### Supported Windows Media Audio File Formats

If you use a Windows Media audio file, consider using low bit rates, and verify the performance of your system under load.

You can use the Microsoft Expression Encoder 4 to convert a file to the Windows Media Audio format. To download Expression Encoder 4, see <https://go.microsoft.com/fwlink/p/?linkid=202843>.

#### Response Group Configuration Tool Requirements

The Response Group Configuration Tool supports the combinations of operating systems and web browsers described in the following table.

##### NOTE

32-bit or 64-bit versions of the operating systems are supported. Only 32-bit versions of Internet Explorer are supported.

#### Supported Operating Systems and Web Browsers

OPERATING SYSTEM	WEB BROWSER
Windows Vista with Service Pack (SP) 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows 7 Windows 7 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2008 with Service Pack 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2008 R2 Windows Server 2008 R2 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2012	
Windows Server 2012 R2	

#### Response Group Agent Console

The agent console supports the combinations of operating systems and web browsers described in the following

table.

**NOTE**

32-bit or 64-bit versions of the operating systems are supported. Only 32-bit versions of Internet Explorer are supported.

**Supported Operating Systems and Web Browsers**

OPERATING SYSTEM	WEB BROWSER
Windows Vista with Service Pack (SP) 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows 7 Windows 7 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode) Firefox 10.0 Chrome 18.0
Windows Server 2008 with Service Pack 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2008 R2 Windows Server 2008 R2 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode) Firefox 10.0 Chrome 18.0
Windows Server 2012	
Windows Server 2012 R2	

## Client support

The Response Group application supports the following clients:

- Skype for Business desktop client
- Lync 2013 desktop client
- Lync 2010 desktop client
- Lync 2010 Attendant
- Office Communications Server 2007 R2 Attendant
- Lync Phone Edition

**NOTE**

The Response Group application is not supported on Lync mobile clients.

The specific client that you can use depends on the type of Response Group user that you are:

- **Callers** can call a response group by using any of the clients listed previously, and by using a standard telephone over the public switched telephone network (PSTN).

- **Informal agents** (agents who do not sign into and out of their groups to accept calls) can accept calls by using Attendant, Lync, or Lync Phone Edition. Informal agents are automatically signed into their groups when they sign in to Skype for Business Server by using one of these clients.
- **Formal agents** (agents who must sign into and out of their groups to accept calls) can accept calls by using Skype for Business and accessing the agent console from the menu item, or by using Attendant and accessing the agent console directly from Internet Explorer.

## Capacity planning

The following table describes the Response Group user model that you can use as the basis for capacity planning requirements.

### NOTE

The numbers in the following table assume that you use 16 kHz, mono, 16-bit Wave (.wav) files for all response group audio files. If you use other file formats, such as Windows Media Audio (.wma), the numbers may vary.

### IMPORTANT

Keep in mind that for disaster recovery capacity planning, each pool of a paired pool should be able to handle the workloads for all the response groups in both pools.

### Response Group User Model

METRIC	PER ENTERPRISE EDITION POOL (WITH 8 FRONT END SERVERS)	PER STANDARD EDITION SERVER
Incoming calls per second	16	2
Concurrent calls connected to IVR or MoH	480	60
Concurrent anonymous sessions (without IM)	224	28
Concurrent anonymous sessions (with IM)	64	8
Active agents (formal and informal)	2400	2400
Number of hunt groups	800	800
Number of IVR groups (use speech recognition)	400	400



# Plan for the Announcement application in Skype for Business

5/20/2019 • 3 minutes to read

Planning for the announcement application in Skype for Business Server Enterprise Voice, which configures what to do with phone calls to unassigned phone numbers in your organizations. Includes audio file requirements.

The Skype for Business Server Announcement application enables you to configure the handling of incoming phone calls when the dialed number is valid for your organization, but is not assigned to a user or a phone. You can transfer these calls to a predetermined destination (phone number, SIP URI, or voice mail), or play an audio announcement, or both. The Announcement application helps you avoid the situations in which a caller misdials and hears a busy tone or the SIP client receives an error message. This section includes planning information that is specific to the Announcement application

When you deploy the Announcement application, you need to configure an unassigned number table that determines the action to be taken when someone dials an unassigned number. The unassigned number table contains ranges of phone numbers that are valid for the organization and specifies which Announcement application handles each range. When a caller dials a telephone number that is valid for your organization but is not assigned to anyone, Skype for Business Server looks up the number in the unassigned number routing table, identifies which range the number falls in, and routes the call to the Announcement application specified for that range. The Announcement application answers the call and plays an audio message (if you configured it to do so) and then either disconnects the call or transfers it to a predetermined destination, such as to an operator. You can use Skype for Business Server Management Shell cmdlets to configure multiple audio messages or to transfer destinations.

How you configure the unassigned number table depends on how you want to use it. If you have specific numbers that are no longer in use and you want to play messages that are tailored for each number, you can enter those specific numbers in the unassigned number table. For example, if you changed the number for your customer service desk, you can enter the old customer service number and associate it with an announcement that gives the new number. If you want to play a general message to anyone who calls a number that is not assigned, such as for employees who have left your organization, you can enter ranges for all the valid extensions in your organization. The unassigned number table is invoked whenever the caller dials a number that is not currently assigned.

## Deployment and requirements

The Announcement application is automatically installed with the Response Group application. The Announcement and Response Group applications are standard components of an Enterprise Voice deployment: When you deploy Enterprise Voice, both of these applications are automatically deployed.

### Software requirements

All Front End Servers or Standard Edition servers that run the Announcement application must have the Windows Media Format Runtime installed for servers running Windows Server 2008 R2, or Microsoft Media Foundation for servers running Windows Server 2012 or Windows Server 2012 R2. For Windows Server 2008 R2, the Windows Media Format Runtime is installed as part of Windows Desktop Experience. Windows Media Format Runtime or Microsoft Media Foundation is required for Windows Media Audio (.wma) files that the Announcement application plays for announcements and music.

### Port Requirements

The Announcement application uses **Port 5071** for SIP listening requests.

**NOTE**

This port is the default setting, which you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Skype for Business Server Management Shell documentation.

**Audio File Requirements**

The Announcement application supports Wave (.wav) file format and Windows Media audio (.wma) file format for music and announcements. Audio file requirements for the Announcement application are the same as for the Response Group application. For details, see [Technical Requirements for Response Groups](#).

# Plan for Shared Line Appearance in Skype for Business Server 2015

5/20/2019 • 2 minutes to read

Read this topic to learn how to plan for Shared Line Appearance (SLA) in Skype for Business Server 2015, November 2015 Cumulative Update.

Shared Line Appearance is a feature in Skype for Business for handling multiple calls on a specific number called a shared number. SLA can configure any enterprise voice enabled Skype for Business user as a shared number with multiple lines to respond to multiple calls. The calls are not actually received on the shared number, instead they are forwarded to users that act as delegates for the shared number. Any one of the delegates can pick up the call while the rest of the delegates get a notification on their phone about who picked up the call and which line has become busy as a result. Both the number of lines and the delegates are configurable for a shared number in SLA. In addition, advanced options, such as BusyOption (what happens in a situation when all lines are busy) and MissedCallOption (the case in which none of the delegates pick up a call), can also be configured for a shared number.

SLA is supported only on the following phone devices (it is not supported for Skype for Business clients on computers, mobile phones, or other devices):

- Polycom VVX300 with firmware update 5.4.1
- Polycom VVX400 with firmware update 5.4.1
- Polycom VVX500 with firmware update 5.4.1
- Polycom VVX600 with firmware update 5.4.1

SLA is a new feature in Skype for Business Server, November 2015 Cumulative Update.

For information about deploying SLA, see [Deploy Shared Line Appearance in Skype for Business Server 2015](#).

## Feature List

Setting up an SLA group enables the following:

- All delegates in the group can answer inbound calls to the same shared number. The calls can be PSTN-based or SIP-based.
- Delegates can hold and pick up calls.
- Delegates can transfer calls to a number outside of the SLA group.
- Delegates can see how many calls are currently on the shared number, and view the status of each of those calls.
- You can configure a maximum number of concurrent calls for the shared number. You can also set how you want additional calls to be handled after this maximum is reached. Excess calls can be rejected with a busy signal, forwarded to an alternate number, or forwarded to voice mail.
- You can configure how you want missed calls (calls not picked up after a certain time) to be handled. If you enable voice mail for the group identity, missed calls automatically go to voice mail. If you do not have voice mail enabled for the group identity (shared number), you can choose for missed calls to be rejected with a busy signal, forwarded to an alternate number, or disconnected.



# Plan for Busy Options for Skype for Business Server

5/20/2019 • 4 minutes to read

Read about the Busy Options feature in Skype for Business Server.

Busy Options is a new voice policy introduced in the July 2016 Cumulative Update that allows you to configure how incoming calls are handled when a user is already in a call or conference, or has a call placed on hold. New or incoming calls can be rejected with a busy signal or forwarded to voice mail.

The Busy Options policy is supported for failover and disaster recovery on paired Front End Pools and Survivable Branch Servers (SBS).

This topic describes the features of Busy Options. For information about how to install and configure Busy Options, see [Install and configure Busy Options for Skype for Business Server](#).

## Configuration options

If Busy Options is enabled for the organization, all users in your organization, both Enterprise Voice and non-Enterprise Voice users, can use the following features:

- Busy on Busy - In which new incoming calls will be rejected with a busy signal if the user is busy.
- Voicemail on Busy - In which new incoming calls will be forwarded to voice mail if the user is busy.

The Busy Options feature provides failover capability. If a problem occurs and users fail over to another Front End Server or to another pool in Skype for Business Server, their Busy Options settings will be preserved.

Regardless of how their busy options are configured, users in a call or conference, or those with a call on hold, are not prevented from initiating new calls or conferences.

After configuration, the Busy Options setting is in effect for all the user's Skype for Business call devices and clients. Based on the user's Busy Options settings, the call that is rejected or sent to voice mail would not ring on any of the user's call devices--including Macintosh, Windows Desktop, mobile clients, or IP phones--on which the user is signed in.

Users will see missed-call notifications on their Skype for Business clients and devices, and they will be notified by email as well. Callers whose call was rejected due to Busy on Busy will see a notification in their Skype for Business client stating that the user they attempted to reach is busy on another call.

You can configure the Busy Options feature by using Skype for Business PowerShell cmdlets to:

- Enable or disable Busy Options Voice policy for the Enterprise.
- Administer Busy on Busy or Voicemail on Busy for all the users in the Enterprise.
- Administer Busy on Busy or Voicemail on Busy for all the users homed in a particular Front End pool.
- Administer Busy on Busy or Voicemail on Busy for a list of users.
- Administer Busy on Busy or Voicemail on Busy for a single user.

## Interoperability with Voice applications

Busy Options provides interoperability with the following Voice applications in Skype for Business:

- Response Groups (RGS)

- Busy Options set on Response Group numbers will be ignored by the system; multiple concurrent calls will be allowed.
- The current Attendant routing experience in Response Groups will remain unchanged for the Agents with Busy Options settings.
- The calls coming from Response Groups to the users who are Response Groups Agents will not be throttled by Busy Options settings and the current RGS experience will be maintained.
- The non-RGS related calls to the Agents will be honored by their Busy Options settings.
- Team Call
  - Incoming calls to users who are set up for a Team Call will be prioritized to ignore Busy on Busy and Voicemail on Busy settings.
  - The current Team Call experience will remain unchanged with Busy Options set for the users.
  - The non-Team Call related calls to such users will be honored by their Busy Options settings.
- Boss/Admin Delegation
  - Incoming calls to users who are set up for a Boss/Admin Delegation either as Boss or an Admin will be prioritized to ignore Busy on Busy and Voicemail on Busy settings.
  - The current Boss/Admin Delegation experience will remain unchanged with Busy Options set for the Admins or Boss.
  - The non-Boss/Admin Delegation related calls to Admins will be honored by their Busy Options settings.
- Shared Line Appearance
  - Busy Options settings on user accounts set up for Shared Line Appearance will be ignored.
  - Shared Line Appearance's native Busy on Busy and Voicemail on Busy options will be honored instead.
- Call Parking Service
  - Parked calls that were not retrieved and are ringing back due to timing out will be allowed to ring though to the user who parked the call by the Busy Options.
- Call Conferencing
  - Users in conference calls are considered Busy and new incoming calls will be rejected with a busy signal or forwarded to voice mail according to their Busy Options settings.
  - Users in conferences are not prevented from initiating new calls or conferences by Busy Options.
  - Users in conferences are still able to receive new conference invitations, but new peer-to-peer calls will be rejected according to their Busy Options settings.
- Simultaneous Ring and Call Forwarding

The Busy on Busy feature is not designed to work with Simultaneous Ring and Call Forwarding.

# Plan for Call Via Work in Skype for Business Server

5/20/2019 • 5 minutes to read

Planning for Call Via Work in Skype for Business Server, which enables integration between Skype for Business and your PBX phone system, so that users can use Skype for Business to control their PBX phones.

**Call Via Work** is a new feature in Skype for Business Server which enables you to integrate your Skype for Business solution with your existing PBX phone systems. A user enabled for Call Via Work can click in Skype for Business to call another user, either within your deployment or an external user. The call is completed using the user's PBX phone. This enables a user with a PBX phone to include audio in their rich Skype for Business conversations. In previous versions of Lync Server remote call control was a feature which enabled users to control their PBX phones with Lync Server. In Skype for Business Server, this feature has been replaced with Call Via Work.

Call Via Work enables the following for PBX phone users

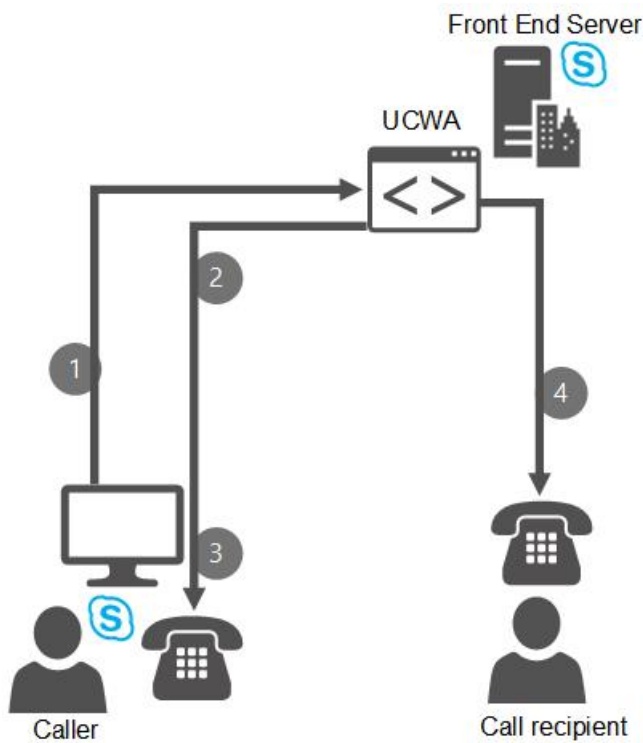
- Click-to-call experience, with the audio provided through the PBX phone.
- Presence, user search, and IM integration-- for example, two Call Via Work users in an IM session can add audio to their session, with the audio provided through the PBX phones.
- The ability to add IM, application sharing, and file transfer to a Call Via Work call.
- One-click meeting join capability

## How it works

Call Via Work uses Unified Communications Web API (UCWA) as the back-to-back user agent (B2BUA) between the PBX system and your Skype for Business Server deployment, so that no computer-supported telecommunications application (CSTA) gateway is needed to connect Skype for Business Server with your PBX system. UCWA is a service introduced in previous versions of Lync Server to enable connectivity with mobile and web clients, and is automatically installed on every Front End Server.

### **Call workflow for a Call Via Work call**

The following illustrates how a user enabled for Call Via Work can use the Skype for Business Server to make a call:



1. The user selects a user in their Skype for Business client, and clicks the phone icon to call them. Or, during an IM conversation, the user clicks to call the user they are having the session with.
2. The PBX phone of the user who placed the call starts to ring. The caller ID for this phone shows a global phone number which you have set up to show in the caller ID of all users placing Call Via Work calls. This global phone number is not an actual phone number that corresponds to any one person's phone. Instead, it is a visual signal to let a user know that this is their own outgoing call, and not an incoming call happening at the same time. When you deploy Call Via Work, you should educate those users about this global phone number and what it means.
3. The user who placed the call picks up their PBX phone. Skype for Business then initiates the voice call to the callee.
4. When the callee answers, the voice call begins. If the two users already had an IM session going, it can continue.

### Joining a Conference With Call Via Work

A Call Via Work user can join a scheduled meeting by clicking the meeting URL. Skype for Business then shows a **Dialing out to** message until the meeting service dials the user's PBX phone. The Call Via Work user then picks up the PBX phone and joins the meeting.

A Call Via Work user can also use the **Meet Now** option in Skype for Business to create Meet Now meetings. The user then sees the **Dialing out to** message, and the PBX phone rings.

A Call Via Work user can also dial in to a meeting by calling the Conference Bridge number from within Skype for Business. If a conference PIN is required, the user must use their PBX phone to input the PIN.

### Incoming Calls

When a user enabled for Call Via Work receives a Skype for Business call, the PBX phone and the user's Skype for Business clients all ring simultaneously (if the user has set up simultaneous ring). The user can accept the call either by picking up the PBX phone or clicking **Accept** on the Skype for Business notification. If the user accepts the call using Skype for Business, the Skype for Business window for the call stays open. But if the user accepts the call by picking up the PBX phone, then the Skype for Business notification window closes and there is no Skype for Business session, only the voice call over the PBX phone.



When a user enabled for Call Via Work receives a PBX call, only the PBX phone rings.

## Limitations of Call Via Work

Call Via Work is a voice solution that requires little hardware setup, but has limitations compared to the features available in full Enterprise Voice or remote call control. Call Via Work has the following limitations:

- If a Call Via Work user has set up call forwarding to the Call Via Work callback number, and someone tries to invite this user to a meeting by the user's phone number, the invitation will not reach the user. You should educate your users to invite participants to meetings by clicking the name, not the phone number.
- Enhanced 911 capability and malicious call tracing are not available during Call Via Work calls.
- Users enabled for Call Via Work cannot use the delegation, team call, or response group features.
- Users of Call Via Work cannot use Skype for Business to record a meeting, mute or unmute the call, hold or transfer the call, or use call park.
- Users cannot use Call Via Work to access their PBX voicemail messages.
- Users of Call Via Work cannot escalate a session that started as a voice call to a collaborative meeting that includes communications such as video, Powerpoint, whiteboard, or One Note.
- Users of Call Via Work cannot add more users to a 2-person call.
- No support for deskphone pairing or VDI plugin pairing.
- If a user makes or answers a call using the PBX phone (and not using the Skype for Business window), there will be no log of the call.
- If your PBX system does not support **REFER with Replaces**, the following behavior will happen. While on a Call Via Work call, if the user transfers the ongoing call from the PBX Phone, the call window will not disappear from their Skype for Business window. If the user then closes the call window, the call between the transfer target and the transferee will end.

## Prerequisites for Call Via Work

To enable any users for Call Via Work, you must have some pre-requisites in place. For more information on these prerequisites, and for steps on how to enable users for Call Via Work, see [Deploy Call Via Work in Skype for Business Server 2015](#).

## See also

[Plan for remote call control in Skype for Business](#)

[Deploy Call Via Work in Skype for Business Server 2015](#)

# Plan for remote call control in Skype for Business

5/20/2019 • 2 minutes to read

Remote call control was a feature in previous versions of Lync Server which enabled users to control their PBX phones with Lync Server. In Skype for Business Server, this feature has been replaced with Call Via Work. *In the client versions for Skype for Business Server 2015 and going forward, remote call control is no longer available to configure in the client and has been removed for use.*

Remote call control users in your organization who are homed on Front End Servers running Lync Server can continue to use remote call control, even if they are using a Skype for Business client. However, for any users homed on Skype for Business Server, remote call control is not supported. See the following table for server/client combinations and whether they can support remote call control or Call via Work.

	<b>SKYPE FOR BUSINESS CLIENT WITH SKYPE UI ENABLED</b>	<b>SKYPE FOR BUSINESS CLIENT WITH LYNC UI ENABLED</b>	<b>SKYPE FOR BUSINESS 2016 CLIENT</b>	<b>LYNC 2013 CLIENT</b>	<b>LYNC 2010 CLIENT</b>
Skype for Business Server	Call via Work	1	Call via Work	1	1
Lync Server 2013	Remote Call Control	Remote Call Control	1	Remote Call Control	Remote Call Control
Lync Server 2010	Remote Call Control	Remote Call Control	1	Remote Call Control	Remote Call Control

1. Neither feature is supported.

For more information, see [Remote Call Control](#) in the Lync Server 2013 documentation.

## See also

[Plan for Call Via Work in Skype for Business Server](#)

[Desktop client feature comparison for Skype for Business](#)

[Make a Skype for Business call but use your PBX desk phone for audio](#)

# Plan Cloud Voicemail service for on-premises users

6/15/2019 • 5 minutes to read

## Overview

This article describes benefits, planning considerations, and requirements for implementing the Microsoft Cloud Voicemail service for your on-premises users. For information on configuring Cloud Voicemail, see [Configure Cloud Voicemail service](#).

Cloud Voicemail takes the place of Exchange Unified Messaging (UM) in providing voice messaging functionality for Skype for Business 2019 voice users who have mailboxes on Exchange Server 2019 or Exchange Online. Cloud Voicemail provides the following benefits for both your on-premises and online users:

- Voicemail answering and deposit functionality with enhanced speech transcription
- Access to voicemail in the user's Exchange mailbox by using the Skype for Business Online or Outlook clients
- The ability to use the Office 365 web-based portal to manage voicemail options
- Support for Exchange mailboxes on premises or in the cloud
- Leveraging of existing user greetings from Exchange Online Unified Messaging

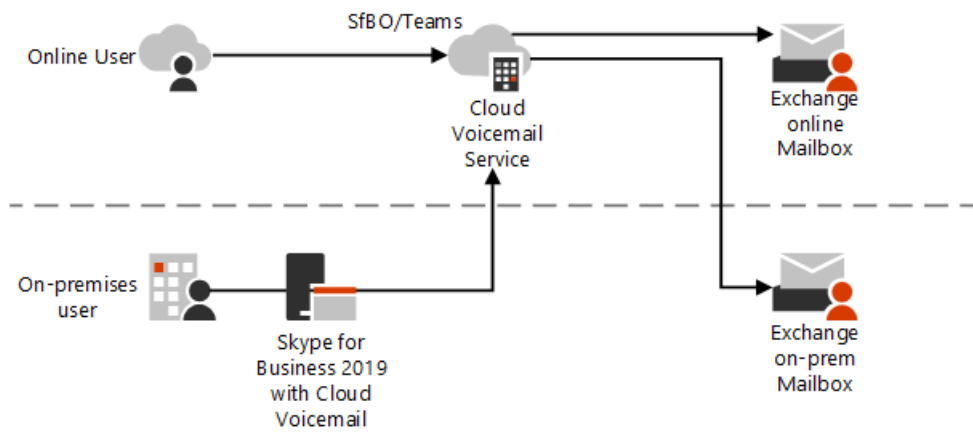
For more information about feature comparison, see [Plan for Skype for Business Server and Exchange Server migration](#).

Skype for Business Server 2019 continues to use Exchange UM for users whose mailboxes are on previous versions of Exchange Server (2013, 2016). Understanding which voicemail solution will be used based on the Exchange Server and Skype for Business Server version is an important part of planning for migration to either Skype for Business Server 2019 or Exchange Server 2019. For more information about migration and interoperability, see [Plan for Skype for Business Server and Exchange Server migration](#).

With Cloud Voicemail, your administration tasks are greatly simplified because:

- There is no need to configure the Exchange UM role.
- The setup tasks for Cloud Voicemail are simpler.
- Updates to voicemail functionality are delivered directly in the cloud, so your users always have access to the latest features and updates with less dependency on Cumulative Updates (CUs).
- You have the same set of controls for both on-premises and online Exchange mailboxes. For more information on these controls, see [Set up Phone System voicemail](#).

The following diagram shows Cloud Voicemail in a hybrid deployment:



Unanswered calls are handled as follows:

1. For users homed in Skype for Business 2019 on premises, unanswered calls are sent by the on-premises Skype for Business Server to the online Cloud Voicemail service.
2. The service processes the voicemail, including transcription.
3. The service then deposits the voicemail in the Exchange mailbox of the user, whether the mailbox is on-premises or online.
4. Users can access their voicemail from either their Skype for Business or Outlook client.

## Requirements

The following requirements assume that you already have Skype for Business Server deployed in a supported topology. Your requirements depend on your scenario:

- If you are already using Exchange UM online and you upgrade to Skype for Business 2019, you will need to modify your hosted voicemail policy and verify that your hosting providers are set correctly. For more information, see [Configure Cloud Voicemail service](#).
- If you are using Exchange UM on premises, or you have a mix of users using Exchange UM online and on premises, you will need modify both your hosted voicemail policy and hosting provider. For more information, see [Configure Cloud Voicemail service](#).
- For a new configuration of Cloud Voicemail, follow the steps outlined in [Configure Cloud Voicemail service](#).

In addition to the requirements above, the below requirements must be configured to connect to the Microsoft Cloud Voicemail service:

- Hybrid connectivity. If you already have Skype for Business Server deployed, and you want to enable Cloud Voicemail for your on-premises users, you must ensure that you have hybrid connectivity set up between your on-premises and online environments. This is sometimes called a split domain configuration.

For more information, see [Plan hybrid connectivity between Skype for Business Server and Office 365](#) and [Configure hybrid connectivity between Skype for Business Server and Office 365](#).

- On-premises users must be enabled for Enterprise Voice and Hosted Voicemail in Skype for Business Server.
- An External Exchange Web Services (EWS) URL and Autodiscover must be set up or some Cloud Voicemail features will be limited.
- If you have an on-premises only deployment—that is, only Exchange and Skype for Business on-premises servers—but you want to take advantage of Cloud Voicemail, you will not need additional licenses.

## Migration and interoperability

If you are planning to deploy Skype for Business Server 2019 and/or Exchange Server 2019, you must plan your migration carefully to ensure continued service for voice messaging. Keep the following in mind:

- Exchange Server 2019 no longer provides Exchange UM functionality
- Skype for Business Server 2019 no longer integrates with Exchange Online UM

Version interoperability and supported topologies for Cloud Voicemail are listed in the following table, which compares the Skype for Business Server versions the user might be homed on with the possible version providing their Exchange Mailbox. Cloud Voicemail only works with Skype for Business Server and Exchange Server 2019 or Exchange Online.

	<b>EXCHANGE SERVER 2013</b>	<b>EXCHANGE SERVER 2016</b>	<b>EXCHANGE SERVER 2019</b>	<b>EXCHANGE ONLINE</b>
Skype for Business Server 2019	Exchange Server UM	Exchange Server UM	Cloud Voicemail	Cloud Voicemail
Skype for Business Server 2015	Exchange Server UM	Exchange Server UM	Cloud Voicemail <sup>1</sup>	Cloud Voicemail Exchange Online UM <sup>2</sup>
Lync Server 2013	Exchange Server UM	Exchange Server UM	Not Supported	Cloud Voicemail Exchange Online UM <sup>2</sup>

<sup>1</sup> Don't see this option yet? It's currently being rolled out and might not be available in your organization yet. See Step 6, Consider opting in, in [Exchange Unified Messaging Online migration support](#) to opt-in for planned connectivity to Cloud Voicemail.

<sup>2</sup> Until deprecated. See [Exchange Unified Messaging Online migration support](#) for more information.

Microsoft recommends the following migration paths:

- If you are upgrading to Skype for Business Server 2019, you can use Exchange UM in Exchange Server 2013 or 2016, but you must upgrade to Cloud Voicemail if you are using Exchange Server 2019.
- If you are upgrading to Exchange Server 2019, and you are using previous versions of Exchange Server UM for Skype for Business Server voice messaging, Microsoft recommends that you upgrade to Skype for Business Server 2019 before the mailbox upgrade. Otherwise, voice messaging capabilities will be lost.
- If you are upgrading to Skype for Business Server 2019, and have Skype for Business Server 2015 configured for voicemail with Exchange Online UM, users' voicemail will automatically migrate from Exchange Online UM to Cloud Voicemail when their account is moved to Skype for Business Server 2019.

For more information about planning your migration, see [Plan for Skype for Business Server and Exchange Server migration](#).

# Configure Cloud Voicemail service for on-premises users

10/21/2019 • 3 minutes to read

## Overview

This article describes how to configure Microsoft Cloud Voicemail service for your Skype for Business on-premises users.

This article assumes that you already have Skype for Business Server deployed in a supported topology, and that you have met the prerequisites for setting up hybrid connectivity.

For more information about the benefits, planning considerations, and requirements for implementing Cloud Voicemail, see [Plan Cloud Voicemail service](#).

Configuring Cloud Voicemail involves the following tasks:

1. Ensure that you have met the prerequisites as described in [Plan Cloud Voicemail service](#).
2. Ensure that you have set up hybrid connectivity as described in [Plan hybrid connectivity](#) and [Configure hybrid connectivity](#).
3. [Configure Cloud Voicemail as the hosting provider on the Edge Server](#) as described in this article.
4. [Configure a hosted voicemail policy](#) as described in this article.
5. [Assign a hosted voicemail policy](#) as described in this article.
6. [Enable a user for Cloud Voicemail](#) as described in this article.

## Configure Cloud Voicemail as the hosting provider on the Edge Server

You configure Cloud Voicemail as the hosting provider on a Front End Server by using the New-CsHostingProvider cmdlet with the following parameters:

- **Identity** specifies a unique string value identifier for the hosting provider that you are creating; for example, Cloud Voicemail.
- **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. This parameter must be set to True.
- **EnabledSharedAddressSpace** indicates whether the hosting provider will be used in a shared SIP address space scenario. This parameter must be set to True.
- **HostsOCSUsers** indicates whether the hosting provider is used to host Skype for Business Server accounts. This parameter must be set to False.
- **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider; for example, proxyserver.contoso.com. Contact your hosting provider for this information. This value cannot be modified. If the hosting provider changes its proxy server, you will need to delete and then re-create the entry for that provider.
- **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Skype for Business Server topology. This parameter must be set to False.

For example, in the Skype for Business Management shell, the following cmdlet configures Cloud Voicemail as the hosting provider:

```
New-CsHostingProvider -Identity "Exchange Online" -Enabled $True -EnabledSharedAddressSpace $True -
HostsOCSUsers $False -ProxyFqdn "exap.um.outlook.com" -IsLocal $False -VerificationLevel UseSourceVerification
```

## Configure a hosted voicemail policy

To ensure that voicemail for your organization is routed to the Cloud Voicemail service, you must configure a hosted voicemail policy for your organization. In many cases, only one hosted voicemail policy is required, and you can modify the global policy to meet all your needs. If your organization requires multiple hosted voicemail policies, you can add policies by using the `new-cshostedvoicemailpolicy` cmdlet.

To modify the global policy, run the following command in the Skype for Business Server management shell after updating your Organization and TenantID:

```
Set-CsHostedVoicemailPolicy -Identity Global -Description "Global Cloud Voicemail Policy" -Destination
exap.um.outlook.com -Organization YourDefaultDomain.onmicrosoft.com -Tenant "11111111-1111-1111-1111-
111111111111"
```

- **Destination** specifies the fully qualified domain name (FQDN) of the hosted Cloud Voicemail service. This value should be set to **exap.um.outlook.com**.
- **Organization** is the default domain assigned to your tenant. You can retrieve this information by having the tenant admin log in to office.com, click on the Admin Center app, navigate to **Setup** on the left, and click **Domains**. For example: mytenant.onmicrosoft.com.

The Organization name is also the Default Domain name in Office 365.

- **Tenant** is used to identify your tenant in Office 365. For more information, see [Find your Office 365 tenant ID](#).

To ensure that a hosted voicemail policy was created successfully, run the following command:

```
Get-CsHostedVoicemailPolicy
```

## Assign a hosted voicemail policy

By default, the Global hosted voicemail policy is assigned to all users. If you use a different policy, before enabling users for hosted voicemail, you must first grant users the desired hosted voicemail policy by using the `Grant-CSHostedVoicemailPolicy` cmdlet.

For example, the following command assigns a non-Global hosted voicemail policy to a user:

```
Get-CsUser -Identity "User1" | Grant-CsHostedVoicemailPolicy -Identity "Tag:CloudVoiceMailUsers"
```

## Enable a user for Cloud Voicemail

To enable a user's voicemail calls to be routed to Cloud Voicemail, you use the `Set-CsUser` cmdlet with the `HostedVoiceMail` parameter.

For example, the following command enables a user account for Cloud Voicemail:

```
Set-CsUser -Identity "User1" -HostedVoiceMail $True
```

The cmdlet verifies that a Cloud Voicemail policy--at the global, site, or user level--applies to this user. If no policy applies, the cmdlet fails.

The next example disables a user account for Cloud Voicemail:

```
Set-CsUser -Identity "User1" -HostedVoiceMail $False
```

The cmdlet verifies that no hosted voicemail policy--at the global, site, or user level--applies to this user. If a policy does apply, the cmdlet fails.

**NOTE**

Users must be enterprise-voice enabled to use the Microsoft Cloud Voicemail Service.



# Plan Cloud auto attendants

8/6/2019 • 5 minutes to read

The auto attendant used with Exchange Unified Messaging (Exchange Server 2013 or Exchange Server 2016) is no longer available in Exchange Server 2019 or Exchange Online. If your implementation of Skype for Business Server 2019 integrates with either of these Exchange versions, you'll need to use the online Cloud Voice features associated with Phone System. See [Plan for Skype for Business Server and Exchange Server migration](#) for information about moving Exchange UM services homed on Exchange server 2013 and 2016 to the cloud.

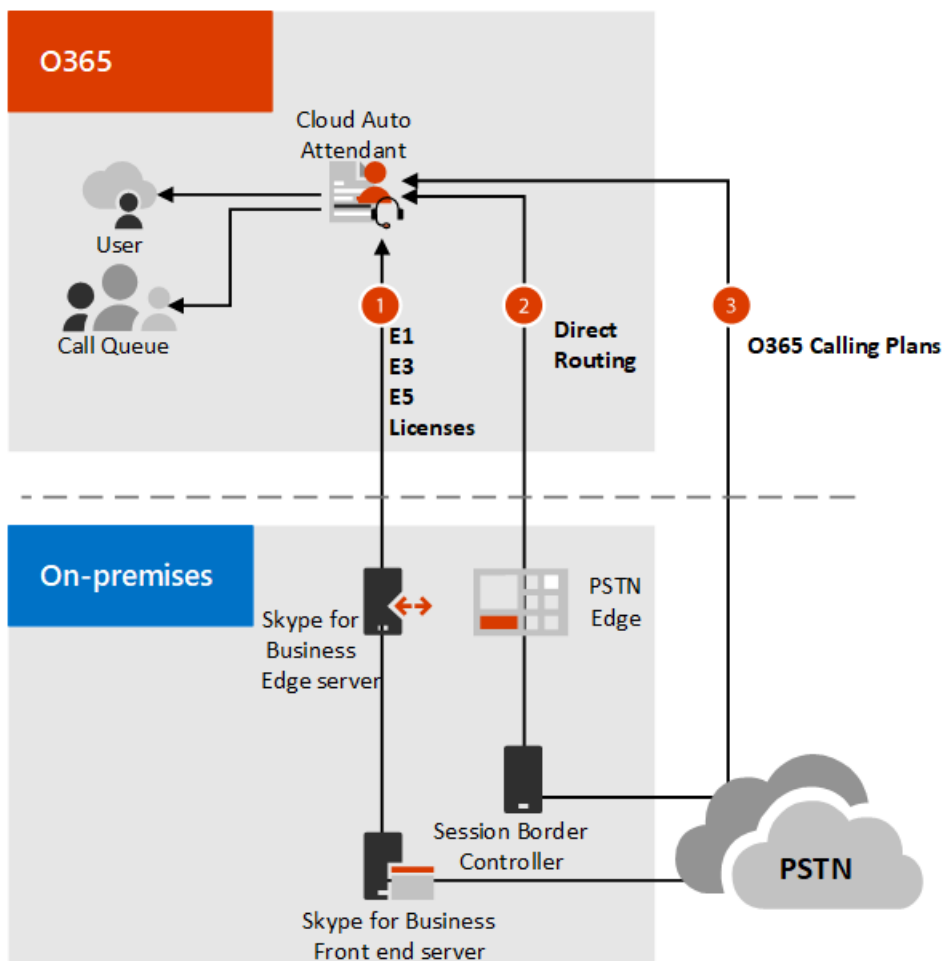
This inherently means that you will have a hybrid implementation of Skype for Business Server 2019 if you wish to use Unified Messaging features like auto attendants. See [Configure hybrid connectivity between Skype for Business Server and Office 365](#) for details.

An Auto attendant is a cloud service that accept customer calls and play greetings, provide them with menu options, and interact with callers using speech or the dialpad to route their calls to the right destination. Each auto attendant is assigned a **resource account** (see [Configure resource accounts](#)) on your Skype for Business Server 2019 system that will be linked directly to an auto attendant in the Microsoft Teams admin center. See [What are Cloud auto attendants?](#) for more detail on what auto attendants are and what options and features exist for auto attendants.

## NOTE

You can assign multiple Microsoft service numbers or hybrid numbers to an auto attendant.

An incoming call to a Cloud auto attendant can take one of several paths, as shown here:



1. Via Skype for Business Server 2019
2. Via a [Session Border Controller](#) and [Direct Routing](#)
3. Via a number homed online in Office 365.

Also see:

- [Set up a Cloud auto attendant](#)
- [Automatically answer and route incoming calls](#)

## Requirements

The following requirements assume that you already have Skype for Business Server 2019 deployed in a supported topology. Your requirements depend on your scenario:

- If you are already using Exchange UM online or on-premises and you upgrade to Skype for Business 2019, you will need to capture the structure of your Auto attendants and re-create them in the cloud using Cloud auto attendants. For more information, see [Moving an Exchange UM auto attendant or call queue to Phone System](#).
- For a new configuration of Cloud auto attendants, follow the steps outlined in [Configure resource accounts](#).

In addition to the requirements above, the below requirements must be configured to connect to the Microsoft Cloud auto attendant service:

- Hybrid connectivity. If you already have Skype for Business Server deployed, and you want to enable Cloud auto attendant for your on-premises users, you must ensure that you have hybrid connectivity set up between your on-premises and online environments. This is sometimes called a split domain configuration.

For more information, see [Plan hybrid connectivity between Skype for Business Server and Office 365](#) and [Configure hybrid connectivity between Skype for Business Server and Office 365](#).

- If you're assigning a phone number to your auto attendant, you will need an [Office 365 Enterprise E5](#) license.
- Create an online [resource account](#) or on-premises [resource account](#) for each auto attendant, and assign phone numbers and licenses.

## Migration and interoperability

If you are planning to deploy Skype for Business Server 2019 and/or Exchange Server 2019, you must plan your migration carefully to ensure continued support for auto attendants. Keep the following in mind:

- Exchange Server 2019 no longer provides Exchange UM functionality
- Exchange Unified Messaging is in retirement mode
- Skype for Business Server 2019 no longer integrates with Exchange Online UM

Cloud auto attendants can be configured with Skype for Business Server 2019, 2015, and 2013.

Microsoft recommends the following migration paths:

- If you are upgrading to Skype for Business Server 2019, you can use Exchange UM in Exchange Server 2013 or 2016, but you must upgrade to Cloud auto attendant if you are using Exchange Server 2019.
- If you are upgrading to Exchange Server 2019, and you are using previous versions of Exchange Server UM for Skype for Business Server voice messaging, Microsoft recommends that you upgrade to Skype for Business Server 2019 before the mailbox upgrade. Otherwise, voice messaging capabilities will be lost.

For more information about planning your migration, see [Plan for Skype for Business Server and Exchange Server migration](#).

### **Migrating a previously implemented Exchange UM auto attendant system**

Currently we don't support automated migration to the Cloud of a UM auto attendant system created in Exchange 2013 or 2016. To manually re-create an auto attendant system, you'll need to:

1. Use Exchange admin powershell commands to review the structure of the old auto attendant system, including any nested auto attendants and call queues.
2. Create copies of text-to-speech scripts or recorded messages associated with each UM auto attendant node.
3. Create on premise endpoints for each auto attendant node, including assigning a test phone numbers and licenses to the objects. Note that you now have the ability to assign on-premise phone numbers licenses used by online services like Phone System.
4. Implement a new Cloud auto attendant service with Skype for Business Online and Phone System. See [Configure resource accounts](#) for implementation details. As you do this, upload the text-to-speech scripts or recorded messages associated with each UM auto attendant node.
5. Test the functionality of the Cloud auto attendant.
6. Reassign the phone number assigned to the old Exchange UM auto attendant to the newly created main Cloud auto attendant.

See [Moving an Exchange UM auto attendant or call queue to Phone System](#) for details on these steps.

## Additional planning resources

The tutorial titled [Small business example - Set up an auto attendant](#) goes through the process of gathering information about user needs, planning a structure of auto attendants and users (and possibly call queues), writing the menu prompts, and implementing the plan in the Teams admin center. Review the tutorial and use the exercises there to create your plan.

When you have a solid structure that meets your needs and a script that guides customers efficiently, proceed to

[Configure resource accounts.](#)

**Caution**

As mentioned in [KB4480742](#), moving Exchange UM auto attendants created in Server 2015 to servers running Server 2019 is discouraged. For the time being, you'd have to keep them on a Skype for Business Server 2015 pool running in coexistence mode.

## See Also

[Plan for Skype for Business Server and Exchange Server migration](#)

[Configure resource accounts](#)

[Enable custom prompt recording using the telephone user interface](#)

[What are Cloud auto attendants?](#)

[Set up a Cloud auto attendant](#)

[Exchange UM: Automatically answer and route incoming calls](#)

[Plan hybrid connectivity between Skype for Business Server and Office 365](#)

[Configure hybrid connectivity between Skype for Business Server and Office 365](#)

[KB4480742: Calls to Subscriber Access or auto attendant fail with fast busy and "500 Server Internal" error after moving contact objects to Skype for Business Server 2019](#)

# Configure resource accounts

11/1/2019 • 9 minutes to read

Skype for Business Server 2019 hybrid implementations only use Cloud services provided by Phone System for unified messaging and do not integrate with Exchange Online. In Skype for Business Server 2019 you are now able to use the Cloud call queues and auto attendants described in [Here's what you get with Phone System in Office 365](#).

To use an Phone System auto attendant or call queue with Skype for Business Server 2019, you will need to create resource accounts that act as application endpoints and can be assigned phone numbers, then use the online Teams admin center to configure the call queue or auto attendant. This resource account can be homed online (see [Manage resource accounts in Microsoft Teams](#) to create resource accounts homed online) or on premises as described in this article. Typically you will have multiple Phone System auto attendant or call queue nodes, each of which is mapped to a resource accounts, which can be homed online or in Skype for Business Server 2019.

If you have an existing Exchange UM auto attendant and call queue system, before you switch to Exchange Server 2019 or Exchange online you will need to manually record the details as described below and then implement a completely new system using the Teams admin center.

## Overview

If your Phone System auto attendant or call queue will need a service number, the various dependencies can be met in the following sequence:

1. Obtain a service number
2. Obtain a free Phone System - [Virtual User license](#) or a paid Phone System license to use with the resource account.
3. Create the resource account. An auto attendant or call queue is required to have an associated resource account.
4. Wait for an active directory sync between online and on premises.
5. Assign the Phone System license to the resource account.
6. Assign a service number to the resource account.
7. Create a Phone System call queue or auto attendant.
8. Associate the resource account with an auto attendant or call queue: (New-CsApplicationInstanceAssociation).

If the auto attendant or call queue is nested under a top level auto attendant, the associated resource account only needs a phone number if you want multiple points of entry into the structure of auto attendants and call queues.

To redirect calls to people in your organization who are homed Online, they must have a **Phone System** license and be enabled for Enterprise Voice or have Office 365 Calling Plans. See [Assign Microsoft Teams licenses](#). To enable them for Enterprise Voice, you can use Windows PowerShell. For example run:

```
Set-CsUser -identity "Amos Marble" -EnterpriseVoiceEnabled $true
```

If the Phone system auto attendant or call queue you're creating will be nested and will not need a phone number, the process is:

1. Create the resource account
2. Wait for an active directory sync between online and on premises
3. Create a Phone System auto attendant or call queue
4. Associate the resource account with a Phone System auto attendant or call queue

# Create a resource account with a phone number

Creating a resource account that uses a phone number would require performing the following tasks in the following order:

1. Port or get a toll or toll-free service number. The number can't be assigned to any other voice services or resource accounts.

Before you assign a phone number to a resource account, you will need to get or port your existing toll or toll-free service numbers. After you get the toll or toll-free service phone numbers, they will show up in **Microsoft Teams admin center** > **Voice** > **Phone numbers**, and the **Number type** listed will be listed as **Service - Toll-Free**. To get your service numbers, see [Getting service phone numbers](#) or if you want to transfer an existing service number, see [Transfer phone numbers to Teams](#).

If you are outside the United States, you can't use the Microsoft Teams admin center to get service numbers. Go to [Manage phone numbers for your organization](#) instead to see how to do it from the outside of the United States.

2. Buy a Phone System license. See:

- [Phone System–Virtual User license](#)
- [Office 365 Enterprise E1 and E3](#)
- [Office 365 Enterprise E5](#)
- [Office 365 Enterprise E5 Business Software](#)

3. Create an on-premises resource account by running the `New-CsHybridApplicationEndpoint` cmdlet for each Phone System auto attendant or call queue, and give each one a name, sip address, and so on.

```
New-CsHybridApplicationEndpoint -DisplayName appinstance01 -SipAddress sip:appinstance01@contoso.com -OU "ou=Redmond,dc=litwareinc,dc=com"
```

See [New-CsHybridApplicationEndpoint](#) for more details on this command.

4. (Optional) Once your resource accounts are created, you can either wait for AD to sync between online and on premises, or force a sync and proceed to online configuration of Phone System auto attendant or call queues. To force a sync you would run the following command on the computer running AAD Connect (if you haven't done so already you would need to load `import-module adsync` to run the command):

```
Start-ADSyncSyncCycle -PolicyType Delta
```

See [Start-ADSyncSyncCycle](#) for more details on this command.

5. Assign the Phone System - Virtual User or Phone System license to the resource account. See [Assign Microsoft Teams licenses](#) and [Assign licenses to one user](#).

If you are assigning a phone number to a resource account you can now use the cost-free Phone System - Virtual User license. This provides Phone System capabilities to phone numbers at the organizational level, and allows you to create auto attendant and call queue capabilities.

6. Assign the service number to the resource account. Use the `Set-CsHybridApplicationEndpoint` command to assign a phone number (with the `-LineURI` option) to the resource account.

```
Set-CsHybridApplicationEndpoint -Identity appinstance01@contoso.com -LineURI tel:+14255550100
```

See [Set-CsHybridApplicationEndpoint](#) for more details on this command.

To assign a direct routing or hybrid number to a resource account, use the following cmdlet:

```
Set-CsOnlineApplicationInstance -Identity appinstance01@contoso.com -OnpremPhoneNumber +14250000000
```

The resource account will need an assigned phone number if it will be assigned to a top level auto attendant or call queue. User (subscriber) phone numbers can't be assigned to a resource account, only service toll or toll-free phone numbers can be used.

You can assign a Direct Routing Hybrid number to your resource account. See [Plan Direct Routing](#) for details.

#### NOTE

Direct Routing service numbers assigned to resource accounts for auto attendant and call queues are supported for Microsoft Teams users and agents only.

7. Create the Phone System auto attendant or call queue. See one of the following:

- [Set up a Cloud auto attendant](#)
- [Create a Cloud call queue](#)

8. Associate the resource account with the Phone System auto attendant or call queue you chose previously.

An example of a small business implementation is available in [Small business example - Set up an auto attendant](#) and [Small business example - Set up a call queue](#).

## Create a resource account without a phone number

This section discusses creating a resource account that is homed on premises. Creating a resource account that is homed online is discussed at [Manage resource accounts in Microsoft Teams](#).

These steps are necessary whether you are creating a brand new Phone System auto attendant or call queue structure, or rebuilding structure originally created in Exchange UM.

Log in to the Skype for Business front end server and run the following PowerShell cmdlets:

1. Create an on-premises resource account by running the `New-CsHybridApplicationEndpoint` cmdlet for each Phone System auto attendant or call queue, and give each one a name, sip address, and so on.

```
New-CsHybridApplicationEndpoint -DisplayName appinstance01 -SipAddress sip:appinstance01@litwareinc.com -OU "ou=Redmond,dc=litwareinc,dc=com"
```

See [New-CsHybridApplicationEndpoint](#) for more details on this command.

2. (Optional) Once your resource accounts are created, you can either wait for AD to sync between online and on premises, or force a sync and proceed to online configuration of Phone System auto attendant or call queues. To force a sync you would run the following command on the computer running AAD Connect (if you haven't done so already you would need to load `import-module adsync` to run the command):

```
Start-ADSyncSyncCycle -PolicyType Delta
```

See [Start-ADSyncSyncCycle](#) for more details on this command.

3. Create the Phone System auto attendant or call queue. See one of the following:

- [Set up a Cloud auto attendant](#)

- [Create a Cloud call queue](#)

4. Associate the resource account and the Phone System auto attendant or call queue you chose previously.

An example of a small business implementation is available in [Small business example - Set up an auto attendant](#) and [Small business example - Set up a call queue](#).

## Test the implementation

The best way to test the implementation is to call the number configured for a Phone System auto attendant or call queue and connect to one of the agents or menus. You can also quickly place a test call by using the **Test button** in the admin center Action pane. If you want to make changes to a Phone System auto attendant or call queue, select it and then in the Action pane click **Edit**.

### TIP

If your resource account has difficulties with being assigned to a call queue or auto attendant, see [Known issues for Microsoft Teams](#) and the [How to fix my hybrid application instances](#) section in the Microsoft Teams Blog.

## Moving an Exchange UM auto attendant or call queue to Phone System

Migration from Exchange UM to Phone System will require recreating the call queue and auto attendant structure, directly migrating from one to the other is not supported. To re-implement a set of call queues and auto attendants:

1. Get a list of all Exchange UM auto attendants and call queues by running the following command on the Exchange 2013 or 2016 system while logged in as admin:

```
Get-UMAutoAttendant | Format-List
```

2. For each listed Exchange UM call queue or auto attendant, note its place in the structure, settings, and get copies of associated sound or text-to-speech files (the guid in the output will be the name of a folder where the files are stored). You can get these details by running the command:

```
Get-UMAutoAttendant -Identity MyUMAutoAttendant
```

See [Get-UMAutoAttendant](#) for more details on this command. A complete list of options you might need to capture is at [UMAutoAttendant members](#) but the most important options to note down are:

- Business hours
- Non-business hours
- Language
- Holiday schedule

3. Create new on-premises endpoints as previously described. Assign the top-level auto attendant a temporary number for testing purposes.
4. Configure a Phone System auto attendant or call queue that uses the endpoints as previously described.

You may find it useful to use the exercises in the tutorial titled [Small business example - Set up an auto attendant](#) to create a logical map of the hierarchies in your old Exchange UM system.

5. Test the Phone System auto attendant or call queue.
6. Reassign the phone number linked to the Exchange UM call queue or auto attendant to the corresponding



Phone System auto attendant or call queue.

At this point, if you have already migrated UM Voicemail, you should be in a position to migrate to Exchange Server 2019.

## See Also

[Create a Cloud call queue](#)

[What are Cloud auto attendants?](#)

[Set up a Cloud auto attendant](#)

[Plan Cloud auto attendants](#)

[Plan Cloud call queues](#)

[Plan Cloud Voicemail service for on-premises users](#)

[New-CsHybridApplicationEndpoint](#)

[New-CsOnlineApplicationInstance](#)

[Manage resource accounts in Microsoft Teams](#) - (to create resource accounts homed online)

# Plan Cloud call queues

7/3/2019 • 2 minutes to read

Cloud call queue is a service that accepts customer calls, plays a greeting message, and then places these calls in a wait queue while searching a pre-configured list of agents to answer these calls. You can define the set of agents in mail-enabled distribution lists or security groups. Your organization can have one or many call queues. Call queues are usually used in combination with auto attendants.

In addition, Cloud call queues can provide:

- Music while callers are waiting on hold
- Customized settings for call queue maximum size, timeout, and call handling options

Each call queue is assigned a **resource account** (see [Configure resource accounts](#)) on your Skype for Business Server 2019 system that will be linked directly to a call queue in the Microsoft Teams admin center. See [Create a Cloud call queue](#) for more detail on what call queues are and what options and features exist for call queues.

## NOTE

You can assign multiple phone numbers to a call queue, but they must be Microsoft service numbers or hybrid numbers.

## Requirements

The following requirements assume that you already have Skype for Business Server 2019 deployed in a supported topology. Your requirements depend on your scenario:

- For a new configuration of Cloud call queues, follow the steps outlined in [Configure resource accounts](#). You will need to create resource accounts either online or in Skype for Business Server 2019, and you may also need to associate a phone number with the call queue.

In addition to the requirements above, the below requirements must be configured to connect to the Microsoft Cloud call queue service:

- Hybrid connectivity. If you already have Skype for Business Server deployed, and you want to enable Cloud call queues for your on-premises users, you must ensure that you have hybrid connectivity set up between your on-premises and online environments. This is sometimes called a split domain configuration.

For more information, see [Plan hybrid connectivity between Skype for Business Server and Office 365](#) and [Configure hybrid connectivity between Skype for Business Server and Office 365](#).

- If you are assigning a phone number to a resource account you can now use the cost-free Phone System Virtual User license. This provides Phone System capabilities to phone numbers at the organizational level, and allows you to create auto attendant and call queue capabilities.
- Create an on-premises [resource account](#) for each call queue, and assign a license and phone number if required.

## Additional planning resources

The tutorial titled [Small business example - Set up an auto attendant](#) goes through the process of gathering information about user needs, planning a structure of auto attendants and users (and possibly call queues), writing the menu prompts, and implementing the plan in the Online Admin center. review the tutorial and use the

exercises there t create your plan.

When you have a solid structure that meets your needs and a script that guides customers efficiently, proceed to [Configure resource accounts](#).

## See Also

[Configure resource accounts](#)

[Enable custom prompt recording using the telephone user interface](#)

[What are Cloud auto attendants?](#)

[Set up a Cloud auto attendant](#)

[Plan hybrid connectivity between Skype for Business Server and Office 365](#)

[Configure hybrid connectivity between Skype for Business Server and Office 365](#)

[Manage resource accounts in Microsoft Teams](#)

# Configure resource accounts

11/1/2019 • 9 minutes to read

Skype for Business Server 2019 hybrid implementations only use Cloud services provided by Phone System for unified messaging and do not integrate with Exchange Online. In Skype for Business Server 2019 you are now able to use the Cloud call queues and auto attendants described in [Here's what you get with Phone System in Office 365](#).

To use an Phone System auto attendant or call queue with Skype for Business Server 2019, you will need to create resource accounts that act as application endpoints and can be assigned phone numbers, then use the online Teams admin center to configure the call queue or auto attendant. This resource account can be homed online (see [Manage resource accounts in Microsoft Teams](#) to create resource accounts homed online) or on premises as described in this article. Typically you will have multiple Phone System auto attendant or call queue nodes, each of which is mapped to a resource accounts, which can be homed online or in Skype for Business Server 2019.

If you have an existing Exchange UM auto attendant and call queue system, before you switch to Exchange Server 2019 or Exchange online you will need to manually record the details as described below and then implement a completely new system using the Teams admin center.

## Overview

If your Phone System auto attendant or call queue will need a service number, the various dependencies can be met in the following sequence:

1. Obtain a service number
2. Obtain a free Phone System - [Virtual User license](#) or a paid Phone System license to use with the resource account.
3. Create the resource account. An auto attendant or call queue is required to have an associated resource account.
4. Wait for an active directory sync between online and on premises.
5. Assign the Phone System license to the resource account.
6. Assign a service number to the resource account.
7. Create a Phone System call queue or auto attendant.
8. Associate the resource account with an auto attendant or call queue: (New-CsApplicationInstanceAssociation).

If the auto attendant or call queue is nested under a top level auto attendant, the associated resource account only needs a phone number if you want multiple points of entry into the structure of auto attendants and call queues.

To redirect calls to people in your organization who are homed Online, they must have a **Phone System** license and be enabled for Enterprise Voice or have Office 365 Calling Plans. See [Assign Microsoft Teams licenses](#). To enable them for Enterprise Voice, you can use Windows PowerShell. For example run:

```
Set-CsUser -identity "Amos Marble" -EnterpriseVoiceEnabled $true
```

If the Phone system auto attendant or call queue you're creating will be nested and will not need a phone number, the process is:

1. Create the resource account
2. Wait for an active directory sync between online and on premises

3. Create a Phone System auto attendant or call queue
4. Associate the resource account with a Phone System auto attendant or call queue

## Create a resource account with a phone number

Creating a resource account that uses a phone number would require performing the following tasks in the following order:

1. Port or get a toll or toll-free service number. The number can't be assigned to any other voice services or resource accounts.

Before you assign a phone number to a resource account, you will need to get or port your existing toll or toll-free service numbers. After you get the toll or toll-free service phone numbers, they will show up in **Microsoft Teams admin center** > **Voice** > **Phone numbers**, and the **Number type** listed will be listed as **Service - Toll-Free**. To get your service numbers, see [Getting service phone numbers](#) or if you want to transfer an existing service number, see [Transfer phone numbers to Teams](#).

If you are outside the United States, you can't use the Microsoft Teams admin center to get service numbers. Go to [Manage phone numbers for your organization](#) instead to see how to do it from the outside of the United States.

2. Buy a Phone System license. See:

- [Phone System–Virtual User license](#)
- [Office 365 Enterprise E1 and E3](#)
- [Office 365 Enterprise E5](#)
- [Office 365 Enterprise E5 Business Software](#)

3. Create an on-premises resource account by running the `New-CsHybridApplicationEndpoint` cmdlet for each Phone System auto attendant or call queue, and give each one a name, sip address, and so on.

```
New-CsHybridApplicationEndpoint -DisplayName appinstance01 -SipAddress sip:appinstance01@contoso.com -OU "ou=Redmond,dc=litwareinc,dc=com"
```

See [New-CsHybridApplicationEndpoint](#) for more details on this command.

4. (Optional) Once your resource accounts are created, you can either wait for AD to sync between online and on premises, or force a sync and proceed to online configuration of Phone System auto attendant or call queues. To force a sync you would run the following command on the computer running AAD Connect (if you haven't done so already you would need to load `import-module adsync` to run the command):

```
Start-ADSyncSyncCycle -PolicyType Delta
```

See [Start-ADSyncSyncCycle](#) for more details on this command.

5. Assign the Phone System - Virtual User or Phone System license to the resource account. See [Assign Microsoft Teams licenses](#) and [Assign licenses to one user](#).

If you are assigning a phone number to a resource account you can now use the cost-free Phone System - Virtual User license. This provides Phone System capabilities to phone numbers at the organizational level, and allows you to create auto attendant and call queue capabilities.

6. Assign the service number to the resource account. Use the `Set-CsHybridApplicationEndpoint` command to assign a phone number (with the `-LineURI` option) to the resource account.

```
Set-CsHybridApplicationEndpoint -Identity appinstance01@contoso.com -LineURI tel:+14255550100
```

See [Set-CsHybridApplicationEndpoint](#) for more details on this command.

To assign a direct routing or hybrid number to a resource account, use the following cmdlet:

```
Set-CsOnlineApplicationInstance -Identity appinstance01@contoso.com -OnpremPhoneNumber +14250000000
```

The resource account will need an assigned phone number if it will be assigned to a top level auto attendant or call queue. User (subscriber) phone numbers can't be assigned to a resource account, only service toll or toll-free phone numbers can be used.

You can assign a Direct Routing Hybrid number to your resource account. See [Plan Direct Routing](#) for details.

#### NOTE

Direct Routing service numbers assigned to resource accounts for auto attendant and call queues are supported for Microsoft Teams users and agents only.

7. Create the Phone System auto attendant or call queue. See one of the following:

- [Set up a Cloud auto attendant](#)
- [Create a Cloud call queue](#)

8. Associate the resource account with the Phone System auto attendant or call queue you chose previously.

An example of a small business implementation is available in [Small business example - Set up an auto attendant](#) and [Small business example - Set up a call queue](#).

## Create a resource account without a phone number

This section discusses creating a resource account that is homed on premises. Creating a resource account that is homed online is discussed at [Manage resource accounts in Microsoft Teams](#).

These steps are necessary whether you are creating a brand new Phone System auto attendant or call queue structure, or rebuilding structure originally created in Exchange UM.

Log in to the Skype for Business front end server and run the following PowerShell cmdlets:

1. Create an on-premises resource account by running the `New-CsHybridApplicationEndpoint` cmdlet for each Phone System auto attendant or call queue, and give each one a name, sip address, and so on.

```
New-CsHybridApplicationEndpoint -DisplayName appinstance01 -SipAddress sip:appinstance01@litwareinc.com -OU "ou=Redmond,dc=litwareinc,dc=com"
```

See [New-CsHybridApplicationEndpoint](#) for more details on this command.

2. (Optional) Once your resource accounts are created, you can either wait for AD to sync between online and on premises, or force a sync and proceed to online configuration of Phone System auto attendant or call queues. To force a sync you would run the following command on the computer running AAD Connect (if you haven't done so already you would need to load `import-module adsync` to run the command):

```
Start-ADSyncSyncCycle -PolicyType Delta
```

See [Start-ADSyncSyncCycle](#) for more details on this command.

3. Create the Phone System auto attendant or call queue. See one of the following:
  - [Set up a Cloud auto attendant](#)
  - [Create a Cloud call queue](#)
4. Associate the resource account and the Phone System auto attendant or call queue you chose previously.

An example of a small business implementation is available in [Small business example - Set up an auto attendant](#) and [Small business example - Set up a call queue](#).

## Test the implementation

The best way to test the implementation is to call the number configured for a Phone System auto attendant or call queue and connect to one of the agents or menus. You can also quickly place a test call by using the **Test button** in the admin center Action pane. If you want to make changes to a Phone System auto attendant or call queue, select it and then in the Action pane click **Edit**.

### TIP

If your resource account has difficulties with being assigned to a call queue or auto attendant, see [Known issues for Microsoft Teams](#) and the [How to fix my hybrid application instances](#) section in the Microsoft Teams Blog.

## Moving an Exchange UM auto attendant or call queue to Phone System

Migration from Exchange UM to Phone System will require recreating the call queue and auto attendant structure, directly migrating from one to the other is not supported. To re-implement a set of call queues and auto attendants:

1. Get a list of all Exchange UM auto attendants and call queues by running the following command on the Exchange 2013 or 2016 system while logged in as admin:

```
Get-UMAutoAttendant | Format-List
```

2. For each listed Exchange UM call queue or auto attendant, note its place in the structure, settings, and get copies of associated sound or text-to-speech files (the guid in the output will be the name of a folder where the files are stored). You can get these details by running the command:

```
Get-UMAutoAttendant -Identity MyUMAutoAttendant
```

See [Get-UMAutoAttendant](#) for more details on this command. A complete list of options you might need to capture is at [UMAutoAttendant members](#) but the most important options to note down are:

- Business hours
  - Non-business hours
  - Language
  - Holiday schedule
3. Create new on-premises endpoints as previously described. Assign the top-level auto attendant a temporary number for testing purposes.
  4. Configure a Phone System auto attendant or call queue that uses the endpoints as previously described.

You may find it useful to use the exercises in the tutorial titled [Small business example - Set up an auto attendant](#) to create a logical map of the hierarchies in your old Exchange UM system.

5. Test the Phone System auto attendant or call queue.
6. Reassign the phone number linked to the Exchange UM call queue or auto attendant to the corresponding Phone System auto attendant or call queue.

At this point, if you have already migrated UM Voicemail, you should be in a position to migrate to Exchange Server 2019.

## See Also

[Create a Cloud call queue](#)

[What are Cloud auto attendants?](#)

[Set up a Cloud auto attendant](#)

[Plan Cloud auto attendants](#)

[Plan Cloud call queues](#)

[Plan Cloud Voicemail service for on-premises users](#)

[New-CsHybridApplicationEndpoint](#)

[New-CsOnlineApplicationInstance](#)

[Manage resource accounts in Microsoft Teams](#) - (to create resource accounts homed online)



# Plan to integrate Skype for Business and Exchange

5/20/2019 • 5 minutes to read

**Summary:** Review this topic for information about how to integrate Skype for Business Server with Exchange Server 2016 or Exchange Server 2013.

Before you can integrate Skype for Business Server and Exchange Server, you must ensure that both Exchange Server and Skype for Business Server are fully installed and up and running.

For details about installing Exchange Server, see the Exchange Server Planning and Deployment documentation for your version of Exchange.

After the servers are up and running, you must assign server-to-server authentication certificates to both Skype for Business Server and Exchange Server; these certificates allow Skype for Business Server and Exchange Server to exchange information and to communicate with one another. When you install Exchange Server, a self-signed certificate with the name Microsoft Exchange Server Auth Certificate is created for you. This certificate, which can be found in the local computer certificate store, should be used for server-to-server authentication on Exchange Server. For details about assigning certificates in Exchange Server, see [Configure Mail Flow and Client Access](#).

For Skype for Business Server you can use an existing Skype for Business Server certificate as your server-to-server authentication certificate; for example, your default certificate can also be used as the OAuthTokenIssuer certificate. Skype for Business Server allows you to use any Web server certificate as the certificate for server-to-server authentication provided that:

- The certificate includes the name of your SIP domain in the Subject field.
- The same certificate is configured as the OAuthTokenIssuer certificate on all of your Front End Servers.
- The certificate has a length of at least 2048 bits.

For details about server-to-server authentication certificates for Skype for Business Server, see [Assign a server-to-server authentication certificate to Skype for Business Server](#).

After the certificates have been assigned, you must then configure the autodiscover service on Exchange Server. In Exchange Server, the autodiscover service configures user profiles and provides access to Exchange services when users log on to the system. Users present the autodiscover service with their email address and password; in turn, the services provide the user with information such as:

- Connection information for both internal and external connectivity to Exchange Server.
- The location of the user's Mailbox server.
- URLs for Outlook features such as free/busy information, Unified Messaging, and the offline address book.
- Outlook Anywhere server settings.

The autodiscover service must be configured before you can integrate Skype for Business Server and Exchange Server. You can verify whether or not the autodiscover service has been configured by running the following command from the Exchange Server Management Shell and checking the value of the `AutoDiscoverServiceInternalUri` property:

```
Get-ClientAccessServer | Select-Object Name, AutoDiscoverServiceInternalUri | Format-List
```

If this value is blank, you must assign a URI to the autodiscover service. Typically this URI will look similar to this:

<https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml>

You can assign the autodiscover URI by running a command similar to this:

```
Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri  
"https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml"
```

For details about the autodiscover service, see [Autodiscover Service](#).

After the autodiscover service has been configured, you must then modify the Skype for Business Server OAuth configuration settings; this ensures that Skype for Business Server knows where to find the autodiscover service. To modify the OAuth configuration settings in Skype for Business Server, run the following command from within the Skype for Business Server Management Shell. When running this command, be sure that you specify the URI to the autodiscover service running on your Exchange Server, and that you use **autodiscover.svc** to point to the service location instead of **autodiscover.xml** (which points to the XML file used by the service):

```
Set-CsOAuthConfiguration -Identity global -ExchangeAutodiscoverUrl  
"https://autodiscover.litwareinc.com/autodiscover/autodiscover.svc"
```

#### NOTE

The Identity parameter in the preceding command is optional; that's because Skype for Business Server only allows you to have a single, global collection of OAuth configuration settings. Among other things, that means that you can configure the autodiscover URL by using this slightly-simpler command:

#### NOTE

```
Set-CsOAuthConfiguration-ExchangeAutodiscoverUrl "https://autodiscover.litwareinc.com/autodiscover/autodiscover.svc"
```

#### NOTE

If you are unfamiliar with the technology, OAuth is a standard authorization protocol used by a number of major websites. With OAuth, user credentials and passwords are not passed from one computer to another. Instead, authentication and authorization is based on the exchange of security tokens; these tokens grant access to a specific set of resources for a specific amount of time.

In addition to configuring the autodiscover service, you must also create a DNS record for the service that points to your Exchange Server. For example, if your autodiscover service is located at [autodiscover.litwareinc.com](https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml) you will need to create a DNS record for [autodiscover.litwareinc.com](https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml) that resolves to the fully qualified domain name of your Exchange Server (for example, [atl-exchange-001.litwareinc.com](https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml)).

If you are integrating Skype for Business Server with Exchange Online, your next steps are in [Configure integration between on-premises Skype for Business Server and Outlook Web App](#), otherwise see [Integrate Skype for Business Server with Exchange Server](#).

## Feature support

The following table details the features supported under various combinations of online or on premises for Exchange and Skype for Business.

	<b>EXCHANGE 2016/2013/2010 (ON PREMISES) + SKYPE FOR BUSINESS SERVER (ON PREMISES)</b>	<b>EXCHANGE ONLINE + SKYPE FOR BUSINESS SERVER (ON PREMISES)</b>	<b>EXCHANGE 2010 (ON PREMISES) + SKYPE FOR BUSINESS ONLINE</b>	<b>EXCHANGE 2016/2013(ON PREMISES) + SKYPE FOR BUSINESS ONLINE</b>	<b>EXCHANGE ONLINE + SKYPE FOR BUSINESS ONLINE</b>
Presence in Outlook	Y	Y	Y	Y	Y
Respond via IM, PSTN Call, Skype Call or Video Call from an Outlook email	Y	Y	Y	Y	Y
Schedule and join online meetings through Outlook	Y	Y	Y	Y	Y
Presence in Outlook Web App	Y	Y	N	N	Y
Respond via IM, PSTN Call, Skype Call or Video Call from an OWA email	Y	Y	N	N	Y
Schedule and join online meetings through Outlook Web App	Y	Y	N	N	Y
IM/Presence in Mobile Clients	Y	Y	Y	Y	Y
Join online meetings in Mobile clients	Y	Y	Y	Y	Y
Publish status based on Outlook calendar free/busy information	Y	Y	Y	Y	Y
Contact List (via Unified Contact Store)	Y (need Exchange 2016/2013)	Y	N	N	Y

	<b>EXCHANGE 2016/2013/2010 (ON PREMISES) + SKYPE FOR BUSINESS SERVER (ON PREMISES)</b>	<b>EXCHANGE ONLINE + SKYPE FOR BUSINESS SERVER (ON PREMISES)</b>	<b>EXCHANGE 2010 (ON PREMISES) + SKYPE FOR BUSINESS ONLINE</b>	<b>EXCHANGE 2016/2013(ON PREMISES) + SKYPE FOR BUSINESS ONLINE</b>	<b>EXCHANGE ONLINE + SKYPE FOR BUSINESS ONLINE</b>
High-resolution Contact Photo (Requires Lync 2013 or Skype for Business clients at a minimum. Not supported for LWA, mobile apps, Lync 2010, Lync for Mac, and other older clients.)	Y (need Exchange 2016/2013)	Y	N	Y	Y
Meeting delegation	Y	Y	Y	Y	Y
Missed Conversations history and Call Logs are written to user's exchange mailbox	Y	Y	Y	Y	Y
Archiving Content (IM and Meeting) in Exchange	Y (need Exchange 2016/2013)	Y	N	N	Y
Search archived content	Y (need Exchange 2016/2013)	Y	N	N	Y
Exchange UM Voice Mail	Y	Y	N	N	N
Server Side Conversation History	Y	Y	N	Y	Y

**NOTE**

There is a Cloud Voicemail service which is supported for Skype for Business Online, Skype for Business Server 2019, Skype for Business Server 2015, and Lync Server 2013.

## See also

[Configure integration between on-premises Skype for Business Server and Outlook Web App](#)

[Configure OAuth between Skype for Business Online and Exchange on premises](#)

[Integrate Skype for Business Server with Exchange Server](#)

How to integrate Exchange Server 2013 with Lync Server 2013, Skype for Business Online, or a Lync Server 2013 hybrid deployment

Configure partner applications in Skype for Business Server and Microsoft Exchange Server

# Plan for Exchange Unified Messaging integration in Skype for Business

10/29/2019 • 8 minutes to read

**Summary:** Review this topic while planning to integrate Skype for Business Server with Exchange 2013 or 2016.

Skype for Business Server supports integration with Exchange Unified Messaging (UM) for combining voice messaging and email messaging into a single messaging infrastructure. In Exchange, Exchange Unified Messaging (UM) is one of several Exchange server roles that you can install and configure.

In Microsoft Exchange Server 2013 and 2016, Exchange UM runs as a service on an Exchange Mailbox server. For Skype for Business Server Enterprise Voice deployments, Unified Messaging combines voice messaging and email messaging into a single store that users can access from a telephone (Outlook Voice Access) or a computer. Unified Messaging and Skype for Business Server work together to provide call answering, Outlook Voice Access, and auto-attendant services to users of Enterprise Voice.

## NOTE

Exchange UM remains available in Skype for Business Server 2019 when you integrate Skype for Business 2019 with Exchange 2013 or Exchange 2016. Due to changes in support in Exchange 2019, Exchange UM integration is being de-emphasized in favor of Cloud Voicemail and Cloud Auto Attendant features. See [Plan Cloud Voicemail service](#) and [Plan for Skype for Business Server and Exchange Server migration](#) for more information.

For these features to be supported in an on-premises Exchange UM deployment, you must be running one of the following:

- Microsoft Exchange Server 2010 or latest service pack (Skype for Business Server 2015 only)
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016

## NOTE

Exchange Unified Messaging as previously known is no longer available in Skype for Business Server 2019, which uses Phone System to record voicemail messages and then leave the recording in a user's Exchange mailbox. See [Plan Cloud Voicemail service](#) for more information.

## Features of integrated Unified Messaging and Skype for Business Server

Skype for Business Server, Enterprise Voice uses the Exchange Unified Messaging (UM) infrastructure to provide call answering, call notification, voice access (including voice mail), and auto-attendant services.

- **Call Answering** Call answering is the receiving of voice messages on behalf of users whose calls are not answered or are busy. It includes playing a personal greeting, recording a message, and submitting the message to be queued for delivery to the user's mailbox, which is stored on the Exchange mailbox server.

If a caller leaves a message, the message is routed to the user's Inbox. If a caller chooses not to leave a message, a missed call notification is stored in the user's mailbox. Users can then access their Inbox by using the Microsoft Outlook messaging and collaboration client, Outlook Web Access, the Exchange ActiveSync

technology, or Outlook Voice Access. The subject and priority of calls can be displayed in a way similar to that of email.

- **Outlook Voice Access** Outlook Voice Access enables an Enterprise Voice user to access not just voice mail, but also the Exchange inbox, including email, calendar, and contacts from a telephony interface. The subscriber access number is assigned by an Exchange UM administrator.
- **Auto attendant** Auto attendant is an Exchange UM feature that can be used to configure a phone number that outside users can dial to reach company representatives. In particular, it provides a series of voice prompts that assist an external caller in navigating a menu system. The list of available options is configured on the Exchange UM server by the Exchange UM administrator.
- **Fax Services** Exchange UM includes fax features, which enable users to receive incoming faxes in their Exchange mailboxes. For details, see [Unified Messaging](#) in the Microsoft Exchange Server documentation.

#### NOTE

Fax services provided by the Exchange UM server are not available in Skype for Business Server deployments that are integrated with Microsoft Exchange Server 2010, Exchange 2010 with the latest service pack, Exchange 2013, or Exchange 2016.

## Components and topologies for on-premises Unified Messaging in Skype for Business Server

### Exchange Server Components

To provide the Exchange UM features and services described in [Features of integrated Unified Messaging and Skype for Business Server](#) to Enterprise Voice users in your organization, you must deploy an Microsoft Exchange Mailbox server and Client Access server, which hosts user mailboxes and provides a single storage location for email and voice mail. Exchange UM runs as a service on Exchange Mailbox and Client Access servers.

For details about Exchange UM components in Microsoft Exchange Server 2010, see [Deploying On-Premises Exchange UM to Provide Lync Server 2013 Preview Voice Mail](#).

### Supported Topologies

You can deploy Skype for Business Server and Exchange Unified Messaging (UM) in the same forest or multiple forests. If the deployment spans multiple forests, you must perform the Exchange integration steps for each Exchange UM forest. Furthermore, you must configure each Microsoft Exchange forest to trust the Skype for Business Server forest and the Skype for Business Server forest to trust each Exchange UM forest. In addition to this forest trust, the Exchange UM settings for all users must be set on the user objects in the Skype for Business Server forest.

Skype for Business Server supports the following topologies for Exchange UM integration:

- Single forest
- Single domain (that is, a single forest with a single domain). Skype for Business Server, Microsoft Exchange, and users all reside in the same domain.
- Multiple domain (that is, a root domain with one or more child domains). Skype for Business Server, and Microsoft Exchange servers are deployed in different domains from the domain where you create users. Exchange UM servers can be deployed in different domains from the Skype for Business Server pool they support.
- Multiple forest (that is, resource forest). Skype for Business Server is deployed in a single forest, and then users are distributed across multiple forests. The users' Exchange UM attributes must be replicated over to

the Skype for Business Server forest.

**NOTE**

Exchange can be deployed in multiple forests. Each Exchange organization can provide Exchange UM to its users, or Exchange UM can be deployed in the same forest as Skype for Business Server.

## Guidelines for integrating on-premises Unified Messaging and Skype for Business Server

The following are guidelines and best practices to consider when you deploy Enterprise Voice:

**IMPORTANT**

Exchange Unified Messaging (UM) supports IPv6 only if you are also using UCMA 4.

- Deploy a Skype for Business Server Standard Edition server or a Front End pool.
- Work with Exchange administrators to confirm which tasks each of you will perform to assure a smooth and successful integration.
- Deploy the Exchange Mailbox server roles in each Exchange Unified Messaging (UM) forest where you want to enable users for Exchange UM. For details about installing Exchange server roles, see the Microsoft Exchange Server documentation.

**IMPORTANT**

When Exchange Unified Messaging (UM) is installed, it is configured to use a self-signed certificate. The self-signed certificate does not enable Skype for Business Server and Exchange UM to trust each other, which is why it is necessary to request a separate certificate from a certification authority that both servers trust.

- If Skype for Business Server and Exchange UM are installed in different forests, configure each Exchange forest to trust the Skype for Business Server forest and the Skype for Business Server forest to trust each Exchange forest. Also, set the users' Exchange UM settings on the user objects in the Skype for Business Server forest, typically by using a script or a cross-forest tool, such as Identity Lifecycle Manager (ILM).
- If necessary, install the Exchange Management Console to manage your Unified Messaging servers.
- Obtain valid phone numbers for Outlook Voice Access and auto attendant.
- If you are using a version of Exchange UM earlier than Microsoft Exchange Server 2010 Service Pack 1 (SP1), coordinate names for Exchange UM SIP URI dial plans and Enterprise Voice dial plans.

### Deploying Redundant Exchange UM Servers

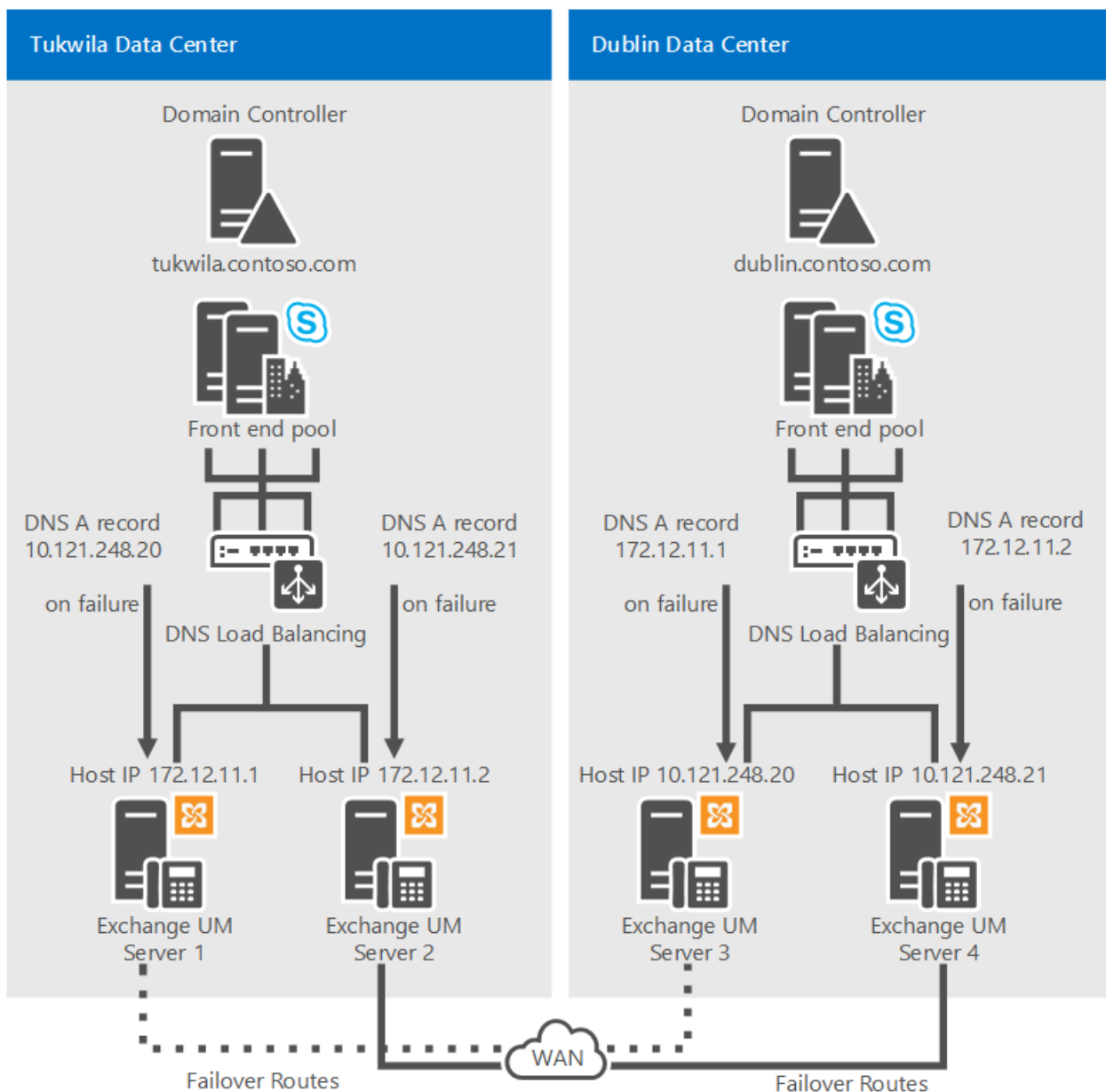
**IMPORTANT**

We recommend that you deploy a minimum of two servers on which Exchange UM services is running for each Exchange UM SIP URI dial plan that you configure for your organization. In addition to providing expanded capacity, deploying redundant servers provides high availability. In the event of an server failure, Skype for Business Server can be configured to fail over to another server.

The following example configurations provide Exchange UM resiliency.

#### Example 1: Exchange UM Resiliency



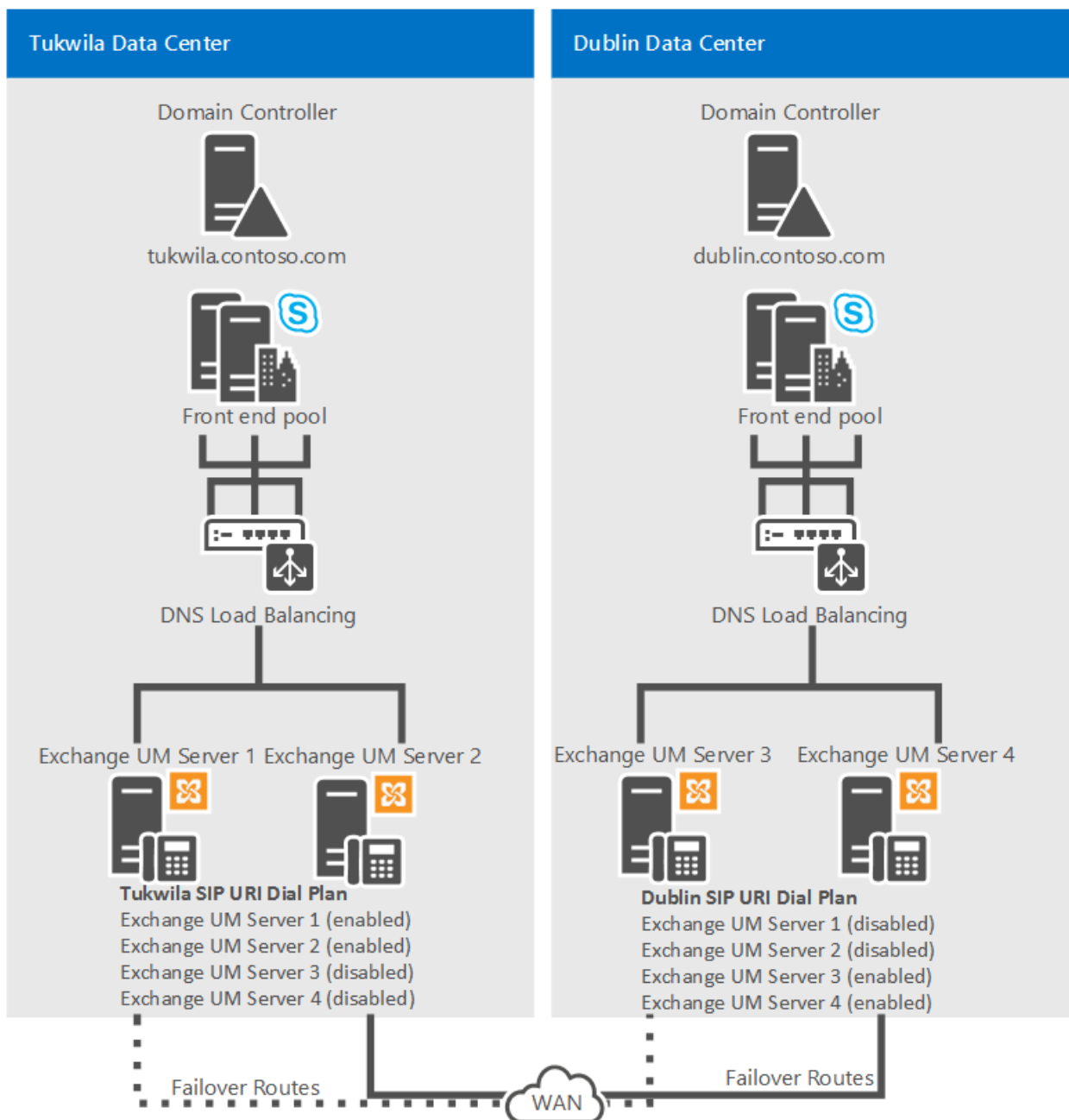


In Example 1, Exchange UM servers 1 and 2 are enabled in the Tukwila data center, and Exchange UM servers 3 and 4 are enabled in the Dublin data center. In the event of an Exchange UM outage in Tukwila, the Domain Name System (DNS) A records for servers 1 and 2 should be configured to point to servers 3 and 4, respectively. In the event of an Exchange UM outage in Dublin, the DNS A records for servers 3 and 4 should be configured to point to servers 1 and 2, respectively.

#### NOTE

For Example 1, you should also assign one of following certificates on each Exchange UM server: either use a certificate with a wildcard in the Subject Alternative Name (SAN) or Put the fully qualified domain name (FQDN) of each of the four Exchange UM servers in the SAN.

### Example 2: Exchange UM Resiliency



In Example 2, under ordinary operating conditions Exchange UM servers 1 and 2 are enabled in the Tukwila data center, and Exchange UM servers 3 and 4 are enabled in the Dublin data center. All four servers are included in the Tukwila users' SIP URI dial plan; however, servers 3 and 4 are disabled. In the event of an Exchange UM outage in Tukwila, for example, Exchange UM servers 1 and 2 should be disabled and Exchange UM servers 3 and 4 should be enabled so the Tukwila Exchange UM traffic will be routed to the servers in Dublin.

For details about how to enable or disable Unified Messaging on Exchange 2013, see [Integrate Exchange 2013 UM with Lync Server](#). The information provided applies equally to Skype for Business Server.

For details about how to enable or disable Unified Messaging on Microsoft Exchange Server 2010, see:

- [Enable Unified Messaging on Exchange 2010](#)
- [Disable Unified Messaging on Exchange 2010](#)

### Exchange Server 2019

Exchange Unified Messaging is no longer present in Exchange 2019, if you have Exchange 2019 and you want equivalent functionality you will need to use the Cloud Voicemail service described in [Plan Cloud Voicemail service](#).

## See also

[Deployment process overview for integrating on-premises Unified Messaging and Skype for Business](#)

# Deployment process overview for integrating on-premises Unified Messaging and Skype for Business

10/16/2019 • 6 minutes to read

**Summary:** Review this topic while planning to integrate Skype for Business Server with Exchange 2013 or 2016.

If you want to integrate Exchange Unified Messaging (UM) with Skype for Business Server, you must perform the tasks outlined in this topic. Also be sure that you review the planning and deployment best practices described in [Plan for Exchange Unified Messaging integration in Skype for Business](#). This topic assumes that you have deployed Skype for Business Server with a collocated Mediation Server and that you have enabled users for Skype for Business Server, but you may not have performed all deployment and configuration steps to enable Enterprise Voice, as described in [Deploy Enterprise Voice in Skype for Business Server](#) in the Deployment documentation.

## NOTE

Exchange Unified Messaging as previously known is no longer available in Skype for Business Server 2019, which uses Phone System to record voicemail messages and then leave the recording in a user's Exchange mailbox. See [Plan Cloud Voicemail service](#) for more information.

## Unified Messaging Integration Process

### IMPORTANT

It is important that you coordinate with your organization's Exchange administrators to confirm the tasks that each of you will perform to help ensure a smooth, successful integration.

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
-------	-------	---------------------------	--------------------------

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
<p>Deploy one of the following:</p> <ul style="list-style-type: none"> <li>• Mailbox</li> </ul> <p>Microsoft Exchange Server 2010 or latest service pack</p> <ul style="list-style-type: none"> <li>• Microsoft Exchange Server 2013</li> <li>• Microsoft Exchange Server 2016</li> </ul>	<p>If you are using Microsoft Exchange Server 2013, install the following Exchange Server roles in either the same forest or a different forest as Skype for Business Server:</p> <ul style="list-style-type: none"> <li>• Client Access</li> <li>• Mailbox</li> </ul> <p>If Microsoft Exchange Server 2013 and Exchange Unified Messaging (UM) are installed in different forests, configure each Exchange forest to trust the Skype for Business Server forest.</p> <p>If you are using Exchange 2010, install the following Exchange Server roles in either the same forest or a different forest as Skype for Business Server:</p> <ul style="list-style-type: none"> <li>• Unified Messaging</li> <li>• Hub Transport</li> <li>• Client Access</li> <li>• Mailbox</li> </ul> <p>If Skype for Business Server and Exchange Unified Messaging (UM) are installed in different forests, configure each Exchange forest to trust the Skype for Business Server forest.</p>	<p>Enterprise administrators (if this is the first Exchange Server in the organization)</p> <p>-OR-</p> <p>Exchange Organization administrator (if this is not the first Exchange Server in the organization)</p>	<p>See the appropriate documentation for your version of Exchange Server:</p> <p>Exchange Server 2010 or latest service pack deployment documentation</p> <p>Exchange Server 2013 Planning and Deployment</p> <p>Exchange Server 2016 Planning and Deployment</p>
<p>Install certificates.</p>	<p>Download and install certificates for each Exchange UM server from a trusted root certificate authority (CA). The certificates are required for mutual Transport Level Security (MTLS) between the servers running Exchange UM and Skype for Business Server.</p>	<p>Administrators</p>	<p><a href="#">Configure certificates on the server running Exchange Server Unified Messaging</a></p>
<p>Create and configure a new Exchange UM SIP dial plan.</p>	<p>On the Exchange UM server, create a SIP dial plan based on your organization's specific deployment requirements.</p>	<p>Exchange Organization administrator</p>	<p><a href="#">Configuring Unified Messaging on Microsoft Exchange Server</a></p>

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
<p>Configure security settings for the Exchange UM SIP dial plan.</p>	<p>To encrypt Enterprise Voice traffic, configure the security settings on the Exchange UM SIP dial plan as <b>SIP Secured</b> or <b>Secured</b>. This is an especially important step if you have deployed or plan to deploy Lync Phone Edition devices in your environment. For Lync Phone Edition devices to function in an environment with Exchange UM integration, Skype for Business Server encryption settings must align with the Exchange UM dial plan security settings. For details, refer to the Deployment documentation.</p>	<p>Exchange Organization administrator</p>	<p>For Exchange 2010 or latest service pack, see also: <a href="#">Configure VoIP Security on a UM Dial Plan</a>. For Exchange 2013, see <a href="#">Unified Messaging</a>.</p>
<p>Add Unified Messaging servers to the Exchange UM SIP dial plan.</p>	<p>To enable a newly installed Unified Messaging server to answer and process incoming calls, you must add the Unified Messaging server to a UM dial plan. In this case, add the server to the Exchange UM SIP dial plan.</p>	<p>Administrators Exchange Server administrators</p>	<p>For Exchange 2010 or latest service pack, see <a href="#">View or Configure the Properties of a UM Server</a>. For Exchange 2013, see <a href="#">Unified Messaging</a>.</p>
<p>Configure mailboxes with SIP addresses.</p>	<p>Assign SIP addresses to the mailboxes of Enterprise Voice users who will be using Exchange UM features.</p>	<p>Skype for Business Server administrator Exchange Recipient administrator</p>	<p>For Exchange 2010 or latest service pack, see <a href="#">Modify a SIP Address for a UM-Enabled User</a>. For Exchange 2013, see <a href="#">Unified Messaging</a>.</p>

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Run the exchucutil.ps1 script.	<p>On the server running Exchange UM services, open the Exchange Management Shell and run the exchucutil.ps1 script, which does the following:</p> <ul style="list-style-type: none"> <li>• Grants Skype for Business Server permission to read Exchange UM Active Directory Domain Services objects, specifically, the SIP dial plans created in the previous task.</li> <li>• Creates a Unified Messaging IP gateway object in Active Directory for each Skype for Business Server Enterprise Edition pool or Standard Edition server that hosts users who are enabled for Enterprise Voice.</li> <li>• Creates an Exchange UM hunt group for each gateway. The hunt group pilot identifier will be the name of the dial plan that is associated with the corresponding gateway. These need to be mapped 1:1 if there is more than one dial plan.</li> </ul>	Exchange Organization administrator Exchange Recipient administrator	<a href="#">Configure Unified Messaging on Microsoft Exchange with ExchUCUtil.ps1</a>
Configure Skype for Business Server dial plans.	<p>If you are integrating with Exchange 2010, create a new Enterprise Voice dial plan with a name that matches the Exchange UM dial plan fully qualified domain name (FQDN).</p> <p><b>Note:</b> You will need to do this for each UM Dial plan. If you are integrating with Exchange 2010 SP1, ensure that suitable global/site-level or pool-level Enterprise Voice dial plans have been configured.</p> <p><b>Note:</b> If you are integrating with Exchange 2010 SP1, the Skype for Business Server dial plan and Exchange UM SIP dial plan names do not need to match.</p>	RTCUniversalServerAdmins	<a href="#">Create or modify a dial plan in Skype for Business Server</a>

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Run the Exchange UM Integration tool.	<p>On the Skype for Business Server, run <b>ocsumutil.exe</b>, which:</p> <ul style="list-style-type: none"> <li>Creates Subscriber Access and Auto Attendant contact objects.</li> <li>Validates that there is an Enterprise Voice dial plan with a name that matches the Exchange UM dial plan FQDN. If you are running Exchange 2010 SP1 or later, the dial plan names do not need to match, and you can ignore the tool's warning about this.</li> <li>This tool works by scanning the Active Directory for Exchange UM settings and allowing the Skype for Business Server administrator to view, create, and edit contact objects.</li> </ul>	<p>RTCUniversalServerAdmins and RTCUniversalUserAdmins</p> <p><b>Important:</b> To run ocsumutil.exe successfully, the user must belong to both of these groups.</p> <p><b>Note:</b> To create Contact objects, the user who runs ocsumutil.exe must have the correct permission to the Active Directory organizational unit (OU) where the new contact objects are stored. This permission can be granted by running the <b>Grant-CsOUPermission</b> cmdlet. For details, see the Skype for Business Server Management Shell documentation.</p>	<p><a href="#">Configure Exchange Server Unified Messaging for Skype for Business Server voice mail</a></p>
If necessary, perform other Enterprise Voice configuration steps.	<p>If you have not already configured Enterprise Voice settings on your servers or users, do one or more of the following:</p> <ul style="list-style-type: none"> <li>• Deploy and configure Public switched telephone network (PSTN) gateways and Mediation Servers</li> <li>• Define voice policies, PSTN usage records, and outbound call routes.</li> <li>• Enable users for Enterprise Voice.</li> <li>• Optionally, configure specific users with dial plans.</li> </ul> <p>Other configuration steps may be required depending on the Enterprise Voice features that you enable.</p>	<p>RTCUniversalServerAdmins RTCUniversalUserAdmins</p>	<p>See topics in the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configure voice policies, PSTN usage records, and voice routes in Skype for Business</a></li> <li>• <a href="#">Deploy Enterprise Voice in Skype for Business Server</a></li> </ul>
Enable Enterprise Voice users for Exchange UM.	<p>On the Exchange UM server, ensure that a Unified Messaging mailbox policy has been created and that each user has a unique extension number assignment, and then enable the user for Unified Messaging.</p>	<p>Exchange Recipient administrator</p>	<p>For Exchange 2010 or latest service pack, see <a href="#">Enable a User for Unified Messaging</a>. For Exchange 2013, see <a href="#">Unified Messaging</a>.</p>

## See also

[Plan for Exchange Unified Messaging integration in Skype for Business](#)



# Plan for unified contact store in Skype for Business Server 2015

5/20/2019 • 2 minutes to read

**Summary:** Review this topic while planning to integrate Skype for Business Server with Exchange 2013 or 2016.

Unified contact store provides a consistent contact experience across Microsoft Office products, and enables users to store all contact information in Exchange 2013 but allows the information to be available globally across Skype for Business, Exchange, Outlook, and Outlook Web Access.

## Requirements for unified contact store

To implement unified contact store in Skype for Business Server:

- You must be running Skype for Business Server and Exchange 2013 or 2016.
- Users must use Skype for Business to migrate their contacts from Skype for Business Server to Exchange 2013 or 2016.
- User mailboxes must be migrated to Exchange 2013.
- You must have server-to-server authentication configured between Skype for Business Server and Exchange 2013 or 2016.

### NOTE

For detailed requirements about setting up authentication between Skype for Business Server and Exchange 2013 or 2016, see [Manage server-to-server authentication \(OAuth\) and partner applications in Skype for Business Server](#) in the Operations documentation.

## See also

[Deploy unified contact store in Skype for Business Server](#)

# Plan for Skype for Business Server and Exchange Server migration

8/7/2019 • 7 minutes to read

This topic covers what you need to consider when you decide to migrate your existing Skype for Business Server or Exchange Server deployments to the latest version or to Skype for Business Online or Exchange Online. What you can migrate, and when, heavily depends on what you've already got set up in your organization. Some features, such as Organization Auto Attendant, aren't available at General Availability (GA) but will be coming later in 2018.

## Feature changes in Exchange 2019 and Skype for Business Server 2019

With Exchange 2019 and Skype for Business Server 2019, we're making some changes to the features we support.

### Unified Messaging support in Exchange 2019

Unified Messaging (UM) has been deprecated in Exchange 2019. This means that Exchange 2019 no longer offers the following features:

- Voicemail
- Auto attendant

If you've deployed the UM role in Exchange 2013 or the UM service in Exchange 2016 and you want to upgrade to Exchange 2019, you'll need to migrate your voicemail to the Microsoft Cloud Voicemail service in Office 365. If you want to migrate your voicemail to Cloud Voicemail, take a look at the [Exchange 2013/Exchange 2016 and Skype for Business 2015 to Exchange 2019 and Skype for Business 2019](#) section below.

#### IMPORTANT

If users on your Exchange 2013 or Exchange 2016 servers have UM-enabled mailboxes, don't move them to Exchange 2019 before you upgrade your Skype for Business servers to Skype for Business Server 2019 and move users to them to avoid a voice messaging outage.

### PBX support in Exchange 2019 and Skype for Business Server 2019

Cloud Voicemail doesn't provide voice messaging functionality to Private Branch Exchanges (PBXs). If you're using Exchange Server Unified Messaging for PBXs and you want to upgrade to Exchange Server 2019, you'll need to adopt one of the three options listed in the blog post [New date for discontinuation of support for Session Border Controllers in Exchange Online Unified Messaging](#) on the [Exchange Team Blog](#).

### Exchange Online UM support in Skype for Business Server 2019

With Skype for Business Server 2019, we're moving from Exchange Online UM to Cloud Voicemail. When a user is moved to a Skype for Business 2019 server, they'll automatically start using Cloud Voicemail when configured for hosted voicemail. If you're currently using Exchange Online UM, you don't need to do anything other than move a user to Skype for Business Server 2019 to start using Cloud Voicemail. However, there are some changes to functionality you need to be aware of:

- Organizational Auto Attendant (the replacement for auto attendant in Exchange Online UM) isn't available at GA but will be available later in 2018.

- User voicemail settings in Outlook on the Web don't apply to Cloud Voicemail.

## On-premises UM migration scenarios

We support the following scenarios that will enable you to migrate users both to Exchange 2019 and to Cloud Voicemail. Later in 2018 we'll support additional scenarios that will let you migrate from additional versions of Exchange and Skype for Business server. We'll also provide additional features such as Organizational Auto Attendant.

- Exchange 2013/Exchange 2016 and Skype for Business Server 2015 to Exchange 2019 and Skype for Business Server 2019
- Skype for Business Server 2015 to Skype for Business Server 2019 with Exchange 2013/Exchange 2016

The following scenarios require that no PBX or SBC configurations exist as part of your current deployment and assume that you have UM configured on your on-premises Exchange servers. Each of these solutions also assumes that you've decided to configure a hybrid deployment between your on-premises Skype for Business servers and Office 365. For more information about Skype for Business hybrid deployments, see [Plan hybrid connectivity](#).

### Exchange 2013/Exchange 2016 and Skype for Business 2015 to Exchange 2019 and Skype for Business 2019

In this scenario, you want to migrate your existing Exchange 2013, Exchange 2016, and Skype for Business 2015 servers to Exchange 2019 and Skype for Business 2019.

As mentioned earlier in this topic, Exchange 2019 no longer includes the UM service. This means that, for any mailboxes that you want to move to Exchange 2019, you need to use Cloud Voicemail to replace the functionality that was provided by the UM service. When you set up Skype for Business Server 2019 and a hybrid deployment between it and Office 365, Cloud Voicemail replaces these Exchange UM voicemail services.

The order in which you move users to Exchange 2019 and Skype for Business Server 2019 is critical to ensuring that voicemail functionality remains available to all users. Where voicemail is processed is also determined by where the Exchange and Skype for Business mailboxes and users are located. Take a look at the following table to see which combinations of Exchange and Skype for Business Server are supported and where voicemail is processed.

MAILBOX LOCATED ON:	USER LOCATED ON SKYPE FOR BUSINESS SERVER 2015	USER LOCATED ON SKYPE FOR BUSINESS SERVER 2019
Exchange 2013/Exchange 2016	Exchange UM	Exchange UM
Exchange 2019	Not supported	Cloud Voicemail

Before you start your migration to Skype for Business Server 2019 and Exchange 2019, keep the following in mind:

- Cloud voicemail doesn't support Organizational Auto Attendant at GA. If you want mailboxes moved to Cloud Voicemail to continue to be available via auto attendant, you'll need to keep at least one Exchange 2013 or Exchange 2016 server running the UM role or service available.
- You need to set up at least one Skype for Business 2019 server **and** move users to that server before you move their mailboxes to Exchange 2019. Failing to do so will result in those mailboxes being unable to receive voicemail messages.
- Calls sent to voicemail will be transferred to Cloud Voicemail where they will be recorded. After the call has ended, the voicemail message will be sent to the recipient's mailbox on the on-premises Exchange 2019 server. You need to take this voice traffic into account when determining whether your Internet connectivity is sufficient to support Cloud Voicemail.

Here are the high-level steps to complete this migration.

1. Install and configure Skype for Business Server 2019 on a new server.
2. Update your hybrid deployment configuration to include the new Skype for Business 2019 server.
3. Install and configure Exchange Server 2019 on a new server.
4. Move users from your Skype for Business 2015 server to your Skype for Business 2019 server.
5. Set the hosted voicemail policy for each user moved to Skype for Business Server 2019 to use Cloud Voicemail.
6. Move mailboxes from your Exchange 2013 or Exchange 2016 server to your Exchange 2019 server.
7. Decommission your Skype for Business 2015 servers after the last user has been moved off of them.
8. Decommission your Exchange 2013 or Exchange 2016 servers after the last mailbox has been moved off of them.

**IMPORTANT**

If you rely on an auto attendant, keep at least one Exchange 2013 or Exchange 2016 running and available.

### **Skype for Business Server 2015 to Skype for Business Server 2019 with Exchange 2013/Exchange 2016**

In this scenario, you want to migrate your existing Skype for Business 2015 server to Skype for Business Server 2019 but remain on Exchange 2013 or Exchange 2016.

When Skype for Business Server 2015 and Skype for Business Server 2019 coexist in the same organization, they work seamlessly with Exchange UM and Cloud Voicemail to ensure that voicemail is correctly delivered to Exchange mailboxes. Whether Exchange UM or Cloud Voicemail processes the voicemail depends on whether the user is located on Skype for Business Server 2015 or Skype for Business Server 2019:

- If a user is located on Skype for Business Server 2015, Exchange UM will process the voicemail message.
- If a user is located on Skype for Business Server 2019, Cloud Voicemail will process the voicemail message.

Regardless of whether Exchange UM or Cloud Voicemail processes the voicemail message, the message will be stored in the user's Exchange mailbox.

Before you start your migration to Skype for Business Server 2019, keep the following in mind:

- Cloud voicemail doesn't support Organizational Auto Attendant at GA. If you want mailboxes moved to Cloud Voicemail to continue to be available via auto attendant, you'll need to keep at least one Exchange 2013 or Exchange 2016 server running the UM role or service available.
- Calls sent to voicemail will be transferred to Cloud Voicemail where they will be recorded. After the call has ended, the voicemail message will be sent to the recipient's mailbox on the on-premises Exchange server. You need to take this voice traffic into account when determining whether your Internet connectivity is sufficient to support Cloud Voicemail.

Here are the high-level steps to complete this migration.

1. Install and configure Skype for Business Server 2019 on a new server.
2. Update your hybrid deployment configuration to include the new Skype for Business 2019 server.
3. Move users from your Skype for Business 2015 server to your Skype for Business 2019 server.
4. Set the hosted voicemail policy for each user moved to Skype for Business Server 2019 to use Cloud Voicemail.

5. Decommission your Skype for Business 2015 servers after the last user has been moved off of them.

**IMPORTANT**

If you rely on an auto attendant, keep at least one Exchange 2013 or Exchange 2016 running and available.

# Exchange Unified Messaging Online migration support

12/7/2019 • 14 minutes to read

In reference to the [announcement](#) on February 8, 2019, Microsoft is retiring the Exchange Unified Messaging Online (ExchUMO) service by February 2020. This article offers a summary of what affected customers should know and do to plan for their business continuity.

ExchUMO is deployed by customers for voicemail, auto attendant, Call Queue, and fax integration services. Microsoft plans to help customers migrate to Phone System services that already support thousands of customers on Skype for Business Online and Microsoft Teams.

Voicemail is primarily a Microsoft-driven migration; admin involvement and/or investment might be required for a subset of customers. Auto attendant is an admin-driven migration; you will need to re-create the existing ExchUMO auto attendant trees in the Cloud Auto Attendant cloud service. Customers who consume any of the ExchUMO features with a third-party PBX will not be migrated to Skype cloud services because they do not support third-party PBX systems. A retirement plan for third-party support was announced in [this blog](#), and customers in this deployment model can migrate their users to one of Microsoft's Unified Communications platforms/services or acquire a third-party voicemail and/or auto attendant solution for these users. Fax integration is not supported in the cloud-based services; customers will need to migrate to a third-party solution.

## Who is affected?

Customers who are consuming any of the following features from Exchange Unified Messaging Online service are affected:

- Voicemail service
- Auto Attendant service
- Call Queue service
- Fax integration

### NOTE

Customers who are using any of the Exchange Server on-premises with Unified Messaging are not affected.

Learn more about the user and admin experience impact in [User experience impact](#).

## Migration plan overview

Microsoft has identified various customer deployments that are consuming features from ExchUMO and will be helping customers migrate based on the following plan.

CUSTOMER GROUP	TIMELINE	DETAILS
----------------	----------	---------

CUSTOMER GROUP	TIMELINE	DETAILS
<p>Customers who are ready to migrate</p> <p>Features to migrate:</p> <ul style="list-style-type: none"> <li>• Voicemail</li> </ul>	March — May 2019	<p>Examples:</p> <ul style="list-style-type: none"> <li>• Customers with simple voicemail deployment and usage</li> <li>• Customers that have all requirements established for Microsoft to execute the migration</li> </ul>
<p>Customers with prerequisites</p> <p>Features to migrate:</p> <ul style="list-style-type: none"> <li>• Voicemail</li> <li>• Auto attendant</li> <li>• Call Queue</li> </ul>	May — December 2019	<p>Examples:</p> <ul style="list-style-type: none"> <li>• Hybrid configuration is not complete</li> <li>• Hybrid PSTN numbers are not set up</li> </ul>
<p>Customers who require admin involvement &amp; customer investment</p> <p>Features to migrate:</p> <ul style="list-style-type: none"> <li>• voicemail</li> <li>• Auto attendant</li> <li>• Call Queues</li> <li>• Fax integration</li> </ul>	By February 2020	<p>Examples:</p> <ul style="list-style-type: none"> <li>• ExchUMO service is consumed by third party PBX</li> <li>• Customers with PSTN Subscriber Access requirements</li> <li>• Customers on SFB 2010 (not-supported)</li> <li>• Fax integration</li> </ul>

## Voicemail migration steps

### 1. Get informed

Familiarize yourself with the [blog announcement](#) and this article to plan a smooth migration for your users. See [Check Skype for Business voicemail and options](#) for details on the Phone System Voicemail capabilities.

### 2. Establish a Skype for Business hybrid topology

If you do not have a Skype for Business hybrid topology established, you need to do that to enable a smooth migration of your voicemail users. See [Configure Skype for Business hybrid](#) for more details.

#### NOTE

You do not need to migrate your users to online for the voicemail service migration. However, for on-premises users to leverage Phone System voicemail service, a hybrid topology is must be established.

### 3. Plan your auto attendant migration

Admins can start migrating their auto attendants from ExchUMO to the Cloud auto attendant at any time. See [Set up a Cloud auto attendant](#) for more details. Microsoft continues to deliver additional auto attendant capabilities that customers may consider required for their migration, admins should evaluate the feature set and migrate their auto attendant instances accordingly. For feature-list comparison, see the [ExchUMO and Azure cloud-based services feature matrix](#).

### 4. Plan for your voicemail post-migration validation and testing

Voicemail migration is Microsoft driven. Admins are not required to do anything, given that the pre-requisite hybrid topology is established. Microsoft performs the required validation and testing to make

sure users' voicemail migration is not disrupted. Admins are encouraged to perform testing and validation on their side. See [Suggested test plan and post-migration validation for admins](#) for a recommended test plan.

#### NOTE

Lync Server 2010 is not supported. If you are in a 2010 server deployment, you should plan a server upgrade or consider migrating your users to Microsoft Teams or Skype for Business Online.

## 5. Monitor the Admin Notification Center

Look out for a notice in the Admin Notification Center with further details and timeline regarding your users' migration. Notifications are sent at least 30 days before your migration period.

#### NOTE

If you received a notification with your users' migration timeline and would like to postpone your migration for a business-critical reason, you can do so by contacting Microsoft Support. Note that you cannot postpone your migration beyond the retirement date, February 2020. For customers who may have more questions, please contact your account team or Microsoft Support. Customers already using Office 365 can submit a support case through the Office 365 Admin portal.

## 6. Consider opting in for a planned migration

You can opt in for a planned Voicemail service migration to CVM. Before opting in, review the details of this article, especially the following sections:

- Migration steps (this section)
- ExchUMO and Azure cloud-based services feature matrix
- User experience impact

When you choose a managed migration you will not receive a pre-migration 30-days notification in the Microsoft 365 admin portal message center.

To opt in for a planned migration, send an email request from your administrator's email address to [cvm@microsoft.com](mailto:cvm@microsoft.com) with the following information:

- Preferred date (Tuesdays): migration waves are executed every Tuesday. Please select a date on a Tuesday that is not beyond 12/3/2019.
- Tenant ID: 32 characters number in this format 0046728c-688a-4472-a38f-098fec60ac6x. You can find your tenant ID in the Microsoft 365 admin portal under Azure AD, or using the following PowerShell cmdlet: `Get-CsTenant | Select ObjectID`

You receive an email confirmation once your tenant is successfully migrated.

## Auto attendant migration guidelines

Office 365 tenant administrators are required to re-create their Exchange UM Online auto attendants in the Microsoft Cloud Auto Attendant service and switch their on-premises phone numbers to them before February 28, 2020, which is when Exchange UMO service will be retired. This is the recommended guideline to successfully migrate and test new Cloud auto attendants. If you have a large number of auto attendants, you can use the [Exchange UM Auto Attendant to Cloud Auto Attendant Migration scripts](#) to simplify the bulk migration of auto attendants.

### Setup



We strongly advise that you start the setup of your new auto attendants early to avoid last minute issues and to get familiar with the functionality and experience of the Cloud Auto Attendant service. For auto attendants that require one or more gap features, you can create and test the auto attendants when the gap features are available to prepare for deployment. For more information about gap features, see the [Appendix](#).

1. Use the Exchange UMO cmdlets to export the configuration of existing auto attendants by using [Get-UMAutoAttendant](#).
2. Use the [Export-UMprompt](#) cmdlet in Exchange Online PowerShell to export the greeting media files (if used) and convert them to .mp3 format.
3. Follow the instructions in [Plan Cloud auto attendants](#) and [Set up a Cloud auto attendant](#) to create auto attendants by using the Microsoft Teams admin center or Powershell.
4. Review your greetings if the menu options changed.
5. Configure transfers to your response groups by using the "Auto Attendant Call Transfer to PSTN" workaround in the [Known issues](#) section of this article.
6. Test the new auto attendants. To test, call them internally or assign a test phone number.

### Cutover

1. Switch your phone numbers from Exchange UMO auto attendants to the new auto attendants.
2. Move the SIP URI from the contact object to the resource account.
3. Test and validate your auto attendants by using the newly-assigned phone numbers.

## Appendix

### ExchUMO and Azure cloud-based services feature matrix

SERVICE	FEATURE LEVEL	FEATURE	NOTES	CLOUD VM/AA	EXUMO
VM	Service Features	Support 3rd-party PBX	Including all features provided to third party PBX such as MWI (Message Waiting Indicator) using SIP notify messages from Exchange UM Online	N	Y
VM	Service Features	Support Skype for Business Server		Y	Y
VM	Service Features	Support Microsoft Teams		Y	N
VM	Service Features	eDiscovery and Hold	For security and compliance	Y	Y
VM	Service Features	Exchange Rules support	For security and compliance	Y	Y
VM	User Features	PSTN Dial-in Access	Subscriber access	N	Y

SERVICE	FEATURE LEVEL	FEATURE	NOTES	CLOUD VM/AA	EXUMO
VM	User Features	PSTN Outlook Voice Access	Subscriber access	N	Y
VM	User Features	Dial-in using an authenticated endpoint	Calling the voicemail service to listen to voice messages and change voicemail settings	Y	Y
VM	User Features	User setting to disable voicemail		Y	Y
VM	User Features	User setting to change the personal greeting		Y	Y
VM	User Features	User setting to create an OOF greeting		Y	Y
VM	User Features	User setting to change the default language		Y	Y
VM	User Features	User setting to overwrite default greeting with TTS		Y	N
VM	User Features	Record personal greetings (authenticated device)		Y	Y
VM	User Features	Record personal greetings (PSTN) — play on phone		N	Y
VM	User Features	User setting to disable transcription		N	Y
VM	User Features	Transcription		Y	Y
VM	User Features	Visual voicemail on all endpoints	With user control to play, delete, message waiting indicator, and status-toggle, on all supported endpoints	Y	Y
VM	User Features	MP3 audio file format in Outlook		Y	Y

SERVICE	FEATURE LEVEL	FEATURE	NOTES	CLOUD VM/AA	EXUMO
VM	User Features	Variable speed play control		Y	Y
VM	User Features	Forward a voicemail	Forward a received voicemail to other users	Y	Y
VM	User Features	Sending a voice message to a group of users	Voicemail broadcast	N	Y
VM	User Features	Voicemail notification using SMS	Users can receive an SMS when they have a new voicemail	N	Y
VM	User Features	Supported greeting languages	Details here: <a href="https://docs.microsoft.com/microsoftteams/what-are-phone-system-auto-attendants">https://docs.microsoft.com/microsoftteams/what-are-phone-system-auto-attendants</a>	Y	Y
VM	User Features	Call answering rules		Y	Y
VM	User Features	Play on phone (PSTN)- to play message	Call me on my cell to listen to the voice message	N	Y
VM	User Features	Play on phone (Auth)- to play message	Call me on my authenticated device	Y	Y
VM	User Features	Shared mailbox between multiple users		Y	Y
VM	Caller Features	Caller experience — protected voicemail	The caller can choose an option to mark a recorded message as protected	N	Y
VM	Caller Features	Caller experience — private voicemail	The caller can choose an option to mark a recorded message as private	N	Y
VM	Caller Features	Silence detection		N	Y

SERVICE	FEATURE LEVEL	FEATURE	NOTES	CLOUD VM/AA	EXUMO
VM	Tenant-Admin Features	Server-level protected voicemail	Tenant-admin can configure a service-level rule to mark incoming voicemail as protected	Y	Y
VM	Tenant-Admin Features	Change recording duration time limit		Y	Y
VM	Tenant-Admin Features	Change silence detection timeout		N/A	Y
VM	Tenant-Admin Features	Change number of input failure	CVM: hard coded to 3	N	Y
VM	Tenant-Admin Features	Change the default language		Y	Y
VM	Tenant-Admin Features	Disable/enable transcription		Y	Y
VM	Tenant-Admin Features	Disable/enable missed call notification		N	Y
VM	Tenant-Admin Features	Help Microsoft improve voice mail preview		Y	Y
VM	Tenant-Admin Features	Customize text message for enabled users		N/A	Y
VM	Tenant-Admin Features	Transcription profanity masking		Y	N
VM	Tenant-Admin Features	Voicemail policy		Y	Y
VM	Tenant-Admin Features	Web portal administration		CY19	Y
VM	Tenant-Admin Features	PowerShell		Y	Y
AA	Service Features	AA support 3rd-party PBX		N	Y
AA	Service Features	Support Skype for Business Server		Y	Y

SERVICE	FEATURE LEVEL	FEATURE	NOTES	CLOUD VM/AA	EXUMO
AA	Service Features	Support Microsoft Teams		Y	N
AA	Service Features	Dial by name, DTMF input		Y	Y
AA	Service Features	Dial by name, speech input		Y	Y
AA	Service Features	Multi-language support	Language details here: <a href="https://docs.microsoft.com/microsoftteams/what-are-phone-system-auto-attendants">https://docs.microsoft.com/microsoftteams/what-are-phone-system-auto-attendants</a>	Y	Y
AA	Service Features	Transfer to operator, CQ, or a user		Y	Y
AA	Service Features	Transfer to PSTN number internally (DID RNL)		Y	Y
AA	Service Features	Transfer to PSTN number externally		Check out Known Issues section below	Y
AA	Service Features	Business hours		Y	Y
AA	Service Features	Menu options	IVR menu options	Y	Y
AA	Service Features	Assigning a cloud PSTN number to AA		Y	N
AA	Service Features	Assigning an on-prem PSTN number to AA		Y	Y
AA	Service Features	Custom user selection	Enabling callers to reach customized list of organization users	Y	Y
AA	Service Features	After-hours and holidays treatment		Y	Y

SERVICE	FEATURE LEVEL	FEATURE	NOTES	CLOUD VM/AA	EXUMO
AA	Service Features	Custom greeting using text to speech		Y	Y
AA	Service Features	Extension dialing	Reaching a user by dialing their extension	Y	Y
AA	Service Features	Mailbox for AA callers to leave a message		CY19	Y
AA	Service Features	Multiple PSTN number assignments to an AA		Y	Y
AA	Tenant-Admin Features	Web portal administration		Y	N
AA	Tenant-Admin Features	PowerShell cmdlets		Y	Y
Fax	Service Features	Fax integration		N	Y

### Suggested test plan and post-migration validation for admins

To validate that your users have been migrated to Cloud Voicemail, leave a voicemail to a user and check the message body in Outlook. Cloud Voicemail messages have a footer that reads:

**Thank you for using Transcription! If you don't see a transcript above, it's because the audio quality was not clear enough to transcribe.**

When testing voicemail functionality after your users have been migrated, make sure to consider the following scenarios:

- Validate voicemail access across all endpoint types in your organization: apps and IP phones.
- Validate with sample users that the configured personalized greetings are played to callers.
- If your organization has a legal or compliance requirement to disable transcription for users, make sure it is disabled post migration. For more details, see [Set up Cloud Voicemail](#).
- If you have previously configured Exchange VM policies and rules, make sure they are effective.
- Familiarize yourself with the Cloud Voicemail service PowerShell cmdlets for changing user settings.

### User experience impact

The following is an overview of end-user voicemail migration experience.

EXPERIENCE	CHANGE IN USER EXPERIENCE
Email notification	No change No email is sent to users notifying them about voicemail account activation/migration.

EXPERIENCE	CHANGE IN USER EXPERIENCE
Access to previous messages	No change Users have access to their previous voicemail messages in all supported endpoints.
Receiving VM in outlook, SFB Apps	No change Users continue to receive their voicemail messages in all supported endpoints.
Transcription	Enhanced CVM transcription has a much higher accuracy rate and supported languages than ExchUMO.
User setting	New experience Users are able to change their preferences from a User Setting Portal (USP). Users can access their USP from a hyperlink in their voicemail email, or the User-Settings button on their SFB client; <a href="https://aka.ms/vmsettings">https://aka.ms/vmsettings</a> .
Features	Please see the feature-set comparison for details.
Outlook rules for VM messages	No change Previously created rules will apply to CVM messages after migration.

#### User management and provisioning in CVM

New Skype for Business users will be automatically provisioned for Cloud voicemail when created. No additional admin work or license is required to provision new voicemail users. See [Set up Cloud Voicemail](#) to learn about policy management for existing and new users.

#### Admin Auto Attendant management experience

To learn more about auto attendants, see [Set up a Cloud auto attendant](#).

#### Known issues

**Auto Attendant Call Transfer to PSTN** Customers are encouraged to configure a temporarily workaround to fulfill the requirements of transferring an auto attendant call to an external PSTN number, or to an RGS instance. An issue was identified during quality assurance with the Transfer out to PSTN number feature, which is not going to be fixed in-time for customers to start migrating off Exchange UMO service before its scheduled retirement date of Feb 1st, 2020. As a workaround, administrators can transfer auto attendant callers to an on-premise virtual user with an active Call Forward setting to the desired PSTN phone number or RGS phone number. Expected Experience

- Administrators do not need to license the virtual user, since this is a workaround solution
- Administrators can manipulate the caller ID that the PSTN receiver will see by assigning the desired number to the virtual user, or using the SBC digit manipulation capabilities
- PSTN Callers will not experience any delay during the call transfer, and they will continue to see the caller ID of the auto attendant after the transfer is successful

**Shared mailbox:** A shared mailbox that is configured using Exchange UM Online will continue to receive messages after being migrated to CVM, and will continue to be accessible to users via Outlook. However, access to change the greeting messages of these mailboxes will not be available once migrated to CVM. Customers with shared mailboxes that are used to capture auto attendant callers should leverage the Auto Attendants and Call Queues Shared Mailbox capabilities once released (ETA October 2019).

**Upgrade to Teams banner on SFB client:** The CVM service is based on Microsoft Teams infrastructure; calls to it from Skype for Business client may cause an information banner to be displayed on the client that reads: "Username is not using Skype for Business. For a richer experience, switch to Teams or start a Skype meeting." Make sure to update your users' Skype for Business client to the latest C2R client update to prevent this banner from appearing.

**Setup your voicemail will take you to OWA:** Clicking on "Set Up Voice Mail" from the client will continue to take Skype for Business Server 2015/2013 customers to the Office Web Access (OWA) portal page after migration to CVM. All settings have been removed from the Voicemail tab in OWA, and a banner will be displayed with a redirect link to take users to the CVM user settings portal.

**Change greeting mobile access:** PSTN subscriber access is not supported in CVM. For users that need to change their greeting remotely, a "Change your greeting" menu option is added to the voicemail IVR service for mobile clients. Users can call this service by pressing and holding the "1" key on the mobile client dial-pad.



# Plan for monitoring in Skype for Business Server

5/20/2019 • 10 minutes to read

**Summary:** Review this topic while planning for the monitoring service in Skype for Business Server.

The monitoring service in Skype for Business Server provides a way for administrators to collect usage and quality data for the communication sessions that take place in their organization, which allows them to identify trends and problems. Ongoing monitoring of your deployment allows you to catch problems early and keep your organization's users satisfied.

Monitoring in Skype for Business Server does not require a separate server role (as was the case in earlier Lync versions); instead, the monitoring service is built into each Front End server. Monitoring is not enabled by default in Skype for Business Server. This article will help you determine whether to enable Monitoring during or after your initial Skype for Business Server configuration, and what SQL resources you'll need to support Monitoring activities. If you're not sure exactly what is or is not monitored and how monitoring can be helpful, go to [Basics about Monitoring](#). To begin your planning process, go to [Define your requirements for monitoring](#). For more details on the SQL requirements for monitoring, go to [SQL requirements for monitoring](#).

## Basics about Monitoring

A session is a generic term for a user's connection to a:

- Conference
- Conferencing tool such as Audio/Video or Application Sharing
- Another user via a peer-to-peer conversation such as instant messaging or an audio call

### NOTE

Skype for Business Server keeps track of information about each session: who called who; which endpoints were used in the session; how long did the session last; what was the perceived quality of the session; and so on. Skype for Business Server does not record and store the actual call itself. That includes instant messaging sessions: although Skype for Business Server records information about instant messaging sessions, it does not maintain a record of each instant message that was sent during the session.

The basic call detail information collected by Skype for Business Server for each session can be used for:

- **Return on Investment (ROI) analysis.** Administrators can compare the usage data to similar data collected for their previous telephony system in order to show cost savings and help justify the deployment of Skype for Business Server.
- **Device Inventory Management.** Asset management information helps administrators identify old devices still in use that need to be replaced, and identify expensive devices that are unused or under-used.
- **Help Desk.** Troubleshooting data helps support engineers determine why a user's call failed, without having to collect server or client side logs. This information can be readily accessed and understood by support personnel who do not have a deep technical knowledge of the Skype for Business client and Skype for Business Server.
- **System Troubleshooting.** Enables administrators to detect major issues that might prevent end users from performing basic tasks like joining a conference, establishing a call, or sending an instant message.

Monitoring also provides a mechanism that allows SIP endpoints (such as Skype for Business) to provide troubleshooting information that the administrator would not otherwise have access to:

- **Media Metrics that Impact Quality.** These metrics deal with the actual transmission of the call itself; they provide a sort of travelogue as the call journeys across the network. These metrics (which include such things as packet loss, jitter, and round trip times) provide information on what happened to the call from the time it left one person's endpoint to the time it arrived at the other person's endpoint.
- **Issues Reported to the End User.** These metrics include poor quality notifications that Skype for Business presents to end users in cases where they are too far from a microphone, speaking too softly, have a poor network connection, or are experiencing poor quality because another program on the computer is consuming the available resources.
- **Environment Information.** These metrics detail call quality factors such as the type of microphone and speakers being used, whether the user is connected through a VPN connection, and whether the user is on a wireless connection.

At the end of each call, SIP-compliant endpoints transmit this information to the Front End server that facilitated the call. You don't have to do anything to get endpoints to transmit that information; that behavior is built into the SIP protocol. However, if you want to collect and store that information, then you need to install and enable monitoring. If you do install and enable monitoring, then call information is gathered by agents running on the Front End server and relayed to a pair of SQL Server databases. The monitoring service (in the form of "unified data collection agents") is collocated into all Front End servers.

## Define your requirements for monitoring

There are still several key issues that should be addressed before you begin to install and configure monitoring with Skype for Business Server:

**When do you want to install monitoring?** Monitoring can be installed and configured at the same time you install and configure Skype for Business Server; the Skype for Business Server Deployment Wizard will provide you with the opportunity to associate your Front End pools with a monitoring database during setup. Alternatively, you can install monitoring after Skype for Business Server itself has been installed; this can be done by using Topology Builder to associate your Front End pools and servers with a monitoring database, and then publishing the revised topology.

Keep in mind that SQL Server must be installed and configured before you deploy and configure monitoring. However, you only need to deploy SQL Server itself; the monitoring databases will be created for you when you publish your Skype for Business Server topology.

**What type of data do you want to monitor?** Skype for Business Server enables you to monitor two general types of data: call detailing recording (CDR) data and Quality of Experience (QoE) data. Call detail recording provides a way for you to track the usage of Skype for Business Server features such as Voice over IP (VoIP) phone calls; instant messaging (IM); file transfers; audio/video (A/V) conferencing; and application sharing sessions. This information helps you know which Skype for Business Server features are being used (and which ones are not) and also provides information as to when these features are being used. Quality of Experience data allows you to maintain a record of the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay).

If you choose to enable monitoring in Skype for Business Server you can enable both CDR monitoring and QoE monitoring, or you can choose to enable one type of monitoring while leaving the other type disabled. For example, suppose your users only use instant messaging and file transfers, and do not make audio or video calls. In that case, there might be little reason to enable QoE monitoring. Likewise, Skype for Business Server makes it easy to enable and disable monitoring after monitoring has been deployed. For example, you might choose to

deploy monitoring but initially leave QoE monitoring disabled. If your users begin to experience problems with audio or video calls you could then enable QoE monitoring and use that data to help you troubleshoot and resolve those problems.

There is no particular advantage (or disadvantage) to installing monitoring at the same time you install Skype for Business Server vs. installing monitoring after Skype for Business Server has been installed. The one point to keep in mind is that, before you install monitoring, you must select a computer to host the backend monitoring store, and a supported version of SQL Server must be installing and configured on that computer before that computer can be used for monitoring. If you have already installed SQL Server on a computer and that computer is ready for use then you can install monitoring at the same time you install Skype for Business Server. If you do not have a backend computer ready then you can proceed to install Skype for Business Server by itself, then install monitoring whenever the backend computer is ready for use.

**How many backend monitoring databases do you need?** It was estimated that a collocated database for both monitoring and archiving could support 240,000 Skype for Business Server users). In addition, a single monitoring database can be used by multiple Front End pools; if you have three Front End pools in your organization then you could associate all three of those pools with the same backend store.

For many organizations, database capacity will not be the deciding factor when determining the number of backend monitoring databases that will be required. Instead, a more important consideration could be network speed. Suppose you have three Front End pools, but one of those pools is located across a slow network connection. In that case, you might want to use two monitoring databases: one database to service the two pools with the good network connection, and a separate database to service the pool with the slower network connection.

You should also take into account that Skype for Business Server supports the use of mirror databases. "Database mirroring" provides a way for you to simultaneously maintain two copies of a database, with each database residing on a different server. Any time data is written to a primary database that same data is also written to the mirror database. If the primary database should fail or otherwise become unavailable, you can "fail over" to the mirror database by using a simple Skype for Business Server PowerShell command. For example:

```
Invoke-CsDatabaseFailover -PoolFqdn atl-cs-001.litwareinc.com -DatabaseType "Monitoring" -NewPrincipal "Mirror"
```

This is important for planning purposes simply because mirroring will require you to double your required number of databases: in addition to each primary database you will need a second database to act as the mirror.

**Do your Skype for Business Server sites need their own custom monitoring configurations?** When you install Skype for Business Server you also install global collections of CDR and QoE configuration settings; these global collections give you the ability to apply the same CDR and QoE settings to your entire organization. In many cases, this will be sufficient: often-times you will want, say, to have CDR monitoring enabled for all of your users.

However, there might also be times when you want to apply different settings to different sites. For example, perhaps you want to use both CDR and QoE monitoring in your Redmond site, but only use CDR monitoring in your Dublin site. Likewise, you might want to retain monitoring data for 60 days in the Redmond site but only need to maintain this type of data for 30 days in the Dublin site. Skype for Business Server allows you to create separate collections of CDR and QoE configuration settings at the site scope; that enables you to manage each site differently. (This includes both enabling and disabling monitoring as well as configuring management settings such as how long data is to be retained.)

Note that you can make this decision before you deploy monitoring or after you deploy monitoring. For example, you can deploy monitoring and then manage the entire organization by using the global settings. If you later change your mind, you can create a separate collection of settings for, say, the Redmond site, and then use those settings to manage monitoring for Redmond. (Settings applied at the site scope always take precedence over

settings applied at the global scope.) If you change your mind again, you can simply delete the configuration settings applied to the Redmond site. When a collection of site settings is removed then the global collection of settings will automatically be applied to that site.

## SQL requirements for monitoring

The unified data collection agents are automatically installed and activated on each Front End server when you enable Monitoring. For supported versions of SQL Server and other details, see [Server requirements for Skype for Business Server 2015](#)

Monitoring data can share a SQL Server instance with other types of data. Typically, the call detail recording database (LcsCdr) and the Quality of Experience database (QoEMetrics) share the same SQL instance; it is also common for the two monitoring databases to be in the same SQL instance as the archiving database (LcsLog). About the only real requirement with SQL Server instances is that any one instance of SQL Server is limited to the following:

- One instance of the Skype for Business Server 2015 backend database. (As a general rule, it is not recommended that your monitoring database be collocated in the same SQL instance, or even on the same computer, as the backend database. Although technically possible, you run the risk of the monitoring database using up disk space needed by the backend database.)
- One instance of the call detail recording database.
- One instance of the Quality of Experience database.
- One instance of the archiving database.

In other words, you can't have two instances of the LcsCdr database in the same instance of SQL Server. If you need multiple instances of the LcsCdr database then you need to configure multiple instances of SQL Server.

## See also

[Deploying Monitoring](#)

# Plan for archiving in Skype for Business Server

7/1/2019 • 13 minutes to read

**Summary:** Read this topic to learn how to plan for archiving in Skype for Business Server.

Corporations and other organizations are subject to an increasing number of industry and government regulations that require the retention of specific types of communications. If your organization has such requirements, you can use archiving in Skype for Business Server to archive instant messaging (IM) and conferencing (meeting) communications to help support some of your compliance requirements.

## Archiving components

Skype for Business Server uses the following archiving components:

- **Archiving agents.** Archiving agents (also known as unified data collection agents) are installed and activated automatically on every Enterprise Edition Front End pool and Standard Edition Server. Although archiving agents are activated automatically, no messages are actually captured until archiving is enabled and appropriately configured. By default, archiving is disabled.
- **Archiving data storage.** Data storage for Skype for Business Server can be implemented as Skype for Business Server SQL Server databases, or, if you have an Exchange deployment, integrated with Exchange storage.

Archiving also requires file storage, but archiving uses the same file storage as the Front End Servers or Standard Edition Server.

## Determine your organizations requirements for archiving

To implement archiving, you need to decide how to meet your organization's requirements for archiving by determining the following:

- **Which storage option to use.** You can implement storage in one of two ways or use a combination of both:
  - **Exchange storage.** If you have an Exchange deployment, you can integrate Skype for Business Server and Exchange archiving so that your Skype for Business Server and Exchange archived data are stored together in Exchange. If you enable the Microsoft Exchange integration option, user mailboxes homed on the Exchange Server use Exchange storage for archived data, but only if the mailboxes have been put on In-Place Hold. By default, Microsoft Exchange integration is not enabled.
  - **Skype for Business Server storage.** If you have users who are not homed on Exchange or who have not had their mailboxes put on In-Place Hold, or if you don't want to use Microsoft Exchange integration for any or all users in your deployment, you can deploy Skype for Business Server Archiving databases using SQL Server.
- **When to deploy archiving.** You can deploy archiving as part of your initial Skype for Business Server deployment, or you can add it to an existing deployment. To use Skype for Business Server archiving storage (SQL Server databases), you use Topology Builder to add the databases to your topology, and then publish the topology again. If all your users are homed on Exchange and have their mailboxes put on In-Place Hold, you do not have to update your topology, but only need to enable Microsoft Exchange integration to store archived data in Exchange.

- **Which sites and users in the organization require archiving.** You can configure archiving settings for your entire organization and, optionally, for specific sites, pools, users, and user groups.
- **What content should be archived.** Whether you specify archiving at the global level or for specific sites and users, at each of these levels, you specify whether to enable the following types of content:
  - Peer-to-peer instant messages
  - Conferences (meetings), which are multiparty instant messages
  - Conference content, including uploaded content (for example, handouts) and event-related content (for example, joining, leaving, uploading sharing, and changes in visibility)
  - Whiteboards and polls shared during a conference
- **What content cannot be archived.** The following types of content cannot be archived:
  - Peer-to-peer file transfers
  - Audio/video for peer-to-peer instant messages and conferences
  - Desktop and application sharing for peer-to-peer instant messages and conferences

Skype for Business Server also does not archive Persistent Chat conversations. To archive Persistent Chat conversations, you must enable and configure the Compliance service, which is a component that can be deployed with Persistent Chat Server. For details, see [Plan for Persistent Chat Server in Skype for Business Server 2015](#).

#### NOTE

Persistent chat is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The same functionality is available in Teams. For more information, see [Getting started with your Microsoft Teams upgrade](#). If you need to use Persistent chat, your choices are to either migrate users requiring this functionality to Teams, or to continue using Skype for Business Server 2015.

- **How long archived materials should be retained.** The Archiving database is not intended for long-term retention, and Skype for Business Server does not provide an e-discovery (search) solution for archived data, so data needs to be moved to other storage. Skype for Business Server provides a session export tool that you can use to export archived data, and which creates searchable transcripts of the archived data.

For the global policy, and for each site and user policy that you create, you can specify when to purge archived and exported data. For more information about purging data, see [Manage purging of archived data in Skype for Business Server](#). For more information about using the session export tool, see [Export archived data in Skype for Business Server](#).

- **Whether to archive internal or external communications.** You can enable archiving for internal communications (communications between internal users), external communications (communications that include at least one user outside your internal network), or both. You can specify these options for your entire organization, or you can specify them for specific sites and pools. By default, neither option is enabled.

#### NOTE

Controlling archiving for internal or external communications is only available for Skype for Business Policy. For Exchange-integrated archiving, both internal and external communications are either archived or not archived.

- **Whether to implement critical mode.** If archiving is a requirement for your organization, configuring critical mode will block IM and conferencing sessions in the event of a Skype for Business Server failure that would prevent archiving. For example:
  - A problem with the Skype for Business Server storage service. In this case, IM is blocked for users who are enabled for archiving.
  - An unavailable file share or a problem with the storage service. In this case, all active conferences hosted in the pool at the time of failure are switched to restricted mode and new conferences cannot be activated.

Both IM and conferencing automatically recover after the failures are corrected.

## Choose archiving deployment and configuration options

Archiving is automatically installed on each Front End Server when you deploy the server, but archiving is not enabled until you configure it. How you configure archiving is determined by how you deploy it. You can deploy archiving in one of the following ways:

- Use Microsoft Exchange storage
- Use Skype for Business Server storage

### NOTE

If you implement both Skype for Business Server Archiving databases and enable Microsoft Exchange integration, Exchange policies override Skype for Business Server archiving policies, but only for users who are homed on Exchange and have had their mailboxes put on In-Place Hold. Skype for Business archiving depends on the Microsoft Exchange In-Place Hold policy.

If you deploy archiving for one Front End pool or Standard Edition Server, you should enable it for all other Front End pools and Standard Edition servers in your deployment. If archiving is not enabled on the pool where a conversation or meeting is hosted, all conference data may not be archived. Archiving will still work for IM messages, but conferencing content and events may not be archived.

### NOTE

To enable delegation of administrative tasks while maintaining your organization's security standards, Skype for Business Server uses role-based access control (RBAC). With RBAC, administrative privilege is granted by assigning users to predefined administrative roles. To configure Skype for Business archiving policies and configurations, the user must be assigned to the CsArchivingAdministrator role (unless the configuration is done directly on the server where archiving is deployed, instead of remotely from another computer). For a list of the user rights, permissions, and roles required for archiving deployment, see [Deploy archiving for Skype for Business Server](#).

### NOTE

If you use Microsoft Exchange integration, configuration of Exchange policies requires appropriate administrator rights and permissions. For details, see the Exchange documentation.

### Microsoft Exchange storage

If you choose Microsoft Exchange integration, you use Exchange policies and configurations to control the archiving of Skype for Business Server. You can configure the Microsoft Exchange integration option at the global level, site level, and pool level. If your deployment includes multiple forests, you must synchronize the settings between Skype for Business Server and Exchange. You will need to determine:

- Whether to archive IM, conferencing, or both
- Whether to implement critical mode, which blocks IM and conferencing sessions in case of a Skype for Business Server failure
- Selection of the Microsoft Exchange integration option to use Exchange for storage of archived data

For information about how to configure Exchange In-Place Hold policies and settings to support archiving, see the Exchange product documentation.

### Skype for Business Server storage

If you choose Skype for Business Server storage, you use Skype for Business Server archiving policies and configurations to control how archiving is enabled and implemented. Skype for Business Server storage uses SQL Server databases, so you will need to add the appropriate SQL Server databases to your topology, then configure your archiving policies.

### Add storage databases to your topology

When adding SQL Server storage databases to your topology, you can choose to collocate the Archiving databases with any of the following:

- Monitoring database
- Back-end database of an Enterprise Edition Front End pool

#### NOTE

The server hosting the Archiving database can host other databases. However, when you consider collocating the Archiving database with other databases, be aware that if you are archiving the messages of more than a few users, the disk space needed by the Archiving database can grow very large. For this reason, we do not recommend collocating the Archiving database with the back-end database.

If you collocate the Archiving database with the Monitoring database, back-end database, or both of these databases, you can either use a single SQL instance for any or all of the databases, or you can use a separate SQL instance for each database, with the following limitation: Each SQL instance can contain only a single back-end database, single Monitoring database, and single Archiving database.

For details about collocation of all server roles and databases, see [Topology Basics for Skype for Business Server](#). For details about updating your topology to include storage databases, see [Create and publish new topology in Skype for Business Server](#).

### Determine archiving options and user policies

You will need to determine:

- Whether to enable or disable archiving for internal and external communications
- Whether to archive IM, conferencing, or both
- Whether to implement critical mode, which blocks IM and conferencing sessions in case of a Skype for Business Server failure
- Whether to enable policies for specific users and groups

Skype for Business Server Archiving options can be specified at the following levels.

- **Global level option.** This is the default archiving configuration and applies to your entire deployment. It is created when you deploy Skype for Business Server and, by default, disables archiving for both internal and external communications. You cannot delete this option. If you choose the delete option, the global option is reset to the default settings.



- **Site level options.** You can enable or disable archiving for one or more specific sites by creating and configuring a site-level archiving option for the site. You can delete any site-level archiving option that you create. A site-level archiving option overrides the global option, but only for the site specified in the option.

For example, if you enable archiving for internal and external communications in your global configuration and create a site configuration in which you disable archiving for external communications, only internal communications would be archived for that site. For another example, if you enable archiving for only IM in your global configuration and create a site configuration in which you enable archiving for both IM and conferencing, conferencing would only be archived for the site, not for the remainder of your organization.

- **Pool level options.** You can specify archiving settings for one or more specific pools by creating and configuring a pool-level configuration for the individual pool. A pool-level archiving configuration exists only if you create it. You can modify and delete any pool-level archiving configuration. A pool-level archiving configuration overrides the global configuration and any site archiving configuration you may have created.

For example, assume you enable archiving for IM only in your global configuration, then create a site-level configuration in which you enable archiving for both IM and conferencing, and then create a pool-level configuration in which you enable archiving only for IM. Communications would be archived for both IM and conferencing for all users of the site except the users homed in the pool specified in the pool-level configuration. For all other users in your organization, archiving would be enabled only for IM.

- **User archiving policies.** You can enable or disable archiving for one or more specific users and groups of users by creating, configuring, and applying a user-level archiving policy for the specified users and user groups. You can delete any user-level archiving policy that you create, and you can change which users and group of users the archiving policy applies to. A user-level archiving policy overrides the global policy and any site policies, but only for the users and user groups to whom the policy is applied.

For example, suppose you disable archiving for internal and external communications in your global configuration, create a site-level policy in which you enable archiving for internal and external communications, and then create a user-level policy in which you disable archiving for external communications. Communications would be archived for both external and internal communications for all site users except for the users to whom you apply the user-level policy--for these users only internal communications would be archived.

For details about how to set up initial archiving configurations when you deploy archiving, see [Deploy archiving for Skype for Business Server](#). For details about managing archiving after deployment, see [Manage archiving in Skype for Business Server](#).

## Archiving configuration tools

You control most archiving options by using the Skype for Business Server Control Panel. However, there are a few options available only by using the Skype for Business Server Management Shell. These options include archiving duplicate messages and exporting archived data. For more information about using the Skype for Business Server Control Panel and the Skype for Business Server Management Shell to manage archiving policies, see [Manage archiving in Skype for Business Server](#).

## Access archived data

Access to archived data is dependent on where the data is stored:

- **Microsoft Exchange storage.** If you choose the Exchange integration option, Skype for Business Server deposits the archiving content in the Exchange store for all users who are homed on Exchange, and who have had their mailboxes put on In-Place Hold. Archived data is stored in the user mailboxes Recoverable items folder, which is generally invisible to users, and can only be searched by users with an Exchange

**Discovery Management** role. Exchange enables federated search and discovery, along with SharePoint, if it is deployed. For more details about storage, retention, and discovery of data stored in Exchange, see the Exchange and SharePoint documentation.

- **Skype for Business Server archiving storage.** If you set up Skype for Business Server Archiving databases, Skype for Business Server deposits archiving content in the Skype for Business Server Archiving databases for any users not homed on Exchange, and who have not had their mailboxes put on In-Place Hold. This data is not searchable, but it can be exported to formats that are searchable using other tools. For details about exporting data stored in Archiving databases, see [Export archived data in Skype for Business Server](#).

## For more information

For more information about archiving, see the following topics:

- [Deploy archiving for Skype for Business Server](#)
- [Manage archiving in Skype for Business Server](#)

For more details about how Skype for Business Server and Exchange work together, see [Plan to integrate Skype for Business and Exchange](#).

# Plan for conferencing in Skype for Business Server

5/20/2019 • 13 minutes to read

**Summary:** Read this topic to learn about conferencing features and capabilities in Skype for Business Server.

Conferencing in Skype for Business Server allows users to meet and hold conferences online using their Skype for Business client instead of everyone getting together in the same room. Meeting participants can connect to a meeting with their Skype for Business client for a full audio and video experience, or dial in to a conference using a phone. Conferences also support instant messaging, desktop and application sharing, and interactive white boards.

This topic includes the following sections:

- Conferencing features and capabilities
- Conferencing components
- Conferencing policies
- Support for large meetings
- Determine your organization's needs

## Conferencing features and capabilities

There are four types of conferencing available in Skype for Business Server: web conferencing, audio and video (A/V) conferencing, dial-in conferencing, and instant message (IM) conferencing.

You can choose to enable all conferencing types, or to use only one type, depending on your needs. For example, you could enable all types, including dial-in conferencing, to allow users who are not able to join a conference with a Skype for Business client to call in and participate in the meeting audio from a telephone. When you deploy Skype for Business Server, IM conferencing capabilities are automatically deployed; you specify whether to deploy web, A/V, and dial-in conferencing by using the Topology Builder. For more information, see [Deploy conferencing in Skype for Business Server](#).

The following subsections describe the features and capabilities of each conferencing type.

### Web conferencing

Web conferencing allows meeting attendees to collaborate on documents shared during the meeting, and for the meeting presenter to share applications through the Skype for Business client. Web conferencing provides the following features:

- **Whiteboard and Annotations.** A whiteboard is a blank canvas that can be used for collaboration, with text, ink, drawings and images. Annotations made on whiteboards can be seen by all meeting participants. The whiteboard feature enhances collaboration by enabling meeting participants to discuss ideas, brainstorm, take notes, and so on.
- **Polling.** The polling feature enhances collaboration by enabling presenters to quickly determine participants' preferences. During online meetings and conversations, presenters can use polling to gather anonymous responses from participants. All presenters can see the results and can either hide the results or show them to all attendees.
- **Application sharing and Desktop sharing.** During a conference, the meeting presenter can share their entire desktop, an individual application, or individual monitors in a multi-monitor environment. Aside from

just viewing the content, other participants in the conference can request control of the presenter's screen and, with permission, interact with the content (including scrolling and editing). Meeting participants can also take over as presenter and start sharing content during the meeting.

- **PowerPoint Sharing.** Allows users to share PowerPoint presentations in the meeting through an Office Web Apps server, which allows for:
  - High-resolution displays and support for PowerPoint capabilities, such as animations, slide transitions, and embedded video.
  - Mobile devices can access these presentations.
  - Users with the appropriate permissions can scroll through a PowerPoint presentation independent of the presentation itself. For example, while Ken is presenting his slide show, Heidi can look at any slide she wants to without affecting Ken's presentation.

### Audio and video conferencing

Audio and video conferencing allows for audio and video in the meeting. Audio allows attendees to talk to each other as though they were in the same room. Video enables video display in the Skype for Business client of any attendees or presenters that join the meeting with a web cam or conferencing device that supports video.

Skype for Business Server provides several features that users can use to configure the audio conferencing experience for the user, including the following:

- **Audience mute.** The presenter can use this setting to mute all the audio participants in the conference and put the conference in a state where non-presenters cannot unmute themselves.
- **Conferencing Entry/Exit Announcements.** If you have enabled dial-in conferencing, presenters can use this setting to turn entry and exit announcements on or off to minimize distractions while a conference is in progress.
- **Adding a user by dialing out.** Presenters and attendees that have been given permission, can add PSTN numbers to the conferences and have the conference dial-out to those numbers.

Skype for Business Server provides several features that users can use to configure the video conferencing experience for the user, including the following:

- **Gallery View.** In video conferences that have more than two people, users automatically see everyone in the conference. If the conference has more than five participants, the video of the most active participants appear in the top row and only the photo appears for the other participants. Multiparty video is turned on by default.
- **Panoramic Video.** If a RoundTable video conferencing device is installed in the conferencing room, this feature provides a full 360 degree view of the conference room. The panoramic video strip is only available with RoundTable devices.
- **Presenter only video mode.** Presenters can configure the meeting so that only the video from the presenter is shown. This prevents distractions in large meetings when multiple video streams are available and locking to different sources. This mode also applies to video captured and provided by RoundTable devices.
- **Video Spotlight.** Presenters can configure the meeting so that only the video from a selected participant who is a video source is seen by the other participants in the conference. This mode also applies to video captured and provided by RoundTable devices for panoramic video.

### Dial-in conferencing

Dial-in conferencing allows meeting attendees to join the audio portion of a meeting by calling in to the meeting from a phone. Dial-in conferencing is a subset of audio conferencing and requires additional configuration. For

more information about dial-in conferencing, see [Plan for dial-in conferencing in Skype for Business Server](#) and [Configure dial-in conferencing in Skype for Business Server](#).

### Instant messaging conferencing

Instant messaging (IM) conferencing allows more than two parties to communicate in a single IM session. For details about IM conferencing, see [Plan for instant messaging and presence in Skype for Business Server](#).

## Conferencing components

The components that support conferencing features include the following:

- **Application service.** The Application service provides a platform for deploying, hosting, and managing unified communications (UC) applications. Dial-in conferencing uses two UC applications that require the Application service: Conferencing Attendant and Conferencing Announcement. The Application service is installed and activated by default on every Front End Server in a Front End pool. It is also installed on every Standard Edition server to enable and configure dial-in conferencing.
- **Conferencing Attendant application.** The Conferencing Attendant application is a unified communications application that accepts public switched telephone network (PSTN) calls, plays prompts, and joins the calls to an A/V conference. The Conferencing Attendant application is installed and activated by default when you enable dial-in conferencing.
- **Conferencing Announcement application.** The Conferencing Announcement application is a unified communications application that plays tones and prompts to PSTN participants on certain actions, such as when participants join or leave a conference, participants are muted or unmuted, someone enters the conference lobby, or the conference is locked or unlocked. Conferencing Announcement application also supports dual-tone multi-frequency (DTMF) commands from the phone keypad. The Conferencing Announcement application is automatically installed and activated by default when you enable dial-in conferencing.
- **Dial-in Conferencing Settings page.** The Dial-in Conferencing Settings page displays conference dial-in numbers with their available languages, assigned conference information (that is, for meetings that do not need to be scheduled), and in-conference DTMF controls, and supports management of personal identification number (PIN) and assigned conferencing information. The Dial-in Conferencing Settings page is automatically installed as part of Web Services.
- **Mediation Server and PSTN gateway.** Dial-in conferencing requires a Mediation Server to translate signaling (and media in some configurations) between Skype for Business Server and the PSTN gateway, and a PSTN gateway to translate signaling and media between the Mediation Server and the PSTN gateway. For dial-in conferencing, you must deploy at least one Mediation Server and at least one of the following:
  - PSTN gateway
  - IP-PBX
  - Session Border Controller (SBC) (for an Internet telephony service provider to which you connect by configuring a SIP trunk)

#### NOTE

If you are also deploying Enterprise Voice, Mediation Server and PSTN gateways are part of the Enterprise Voice deployment. If you are not deploying Enterprise Voice, you need to deploy at least one Mediation Server and at least one PSTN gateway, IP-PBX, or SBC for dial-in conferencing.

- **File store.** File store is used for recorded name audio files. File Store is a standard component in every

Enterprise Edition or Standard Edition deployment.

- **User store.** User store is used to store user Skype for Business Server PINs. PINs are hashed. The User store is a standard component in every Enterprise Edition or Standard Edition deployment.
- **Office Web Apps Server.** In order to use web conferencing capabilities, administrators must install Office Web Apps Server and they must configure Skype for Business Server to communicate with Office Web Apps Server.

## Conferencing policies

To enforce your organization's policies and control bandwidth usage, you can set policies for the types of meetings that users can organize. You can define a wide variety of conferencing policies, and assign them to individual users and groups of users. You can also set policies that govern peer-to-peer conversations. For details about setting conferencing policies, see [Manage conferencing policies in Skype for Business Server](#). For details about bandwidth management, see [Plan for call admission control in Skype for Business Server](#).

## Support for large meetings

The size of meetings that Skype for Business Server can support depends on whether conferencing is hosted on a shared or dedicated pool:

- On a shared pool, Skype for Business Server can host meetings with up to 250 users. A shared pool is a pool that hosts all Skype for Business Server workloads including instant messaging (IM) and presence, conferencing, and Enterprise Voice.
- On a dedicated pool, Skype for Business Server can support meetings with up to 1000 participants using web and audio/video (A/V) conferencing, including sharing PowerPoint presentations. This support requires a dedicated pool configured to support large meetings and managed in a way that ensures hosting of only a single large meeting at a time.

For more information about managing large meetings, see [Plan for large meetings in Skype for Business Server](#).

If your organization requires larger meeting capabilities, you should consider implementing a hybrid environment that takes advantage of Skype Meeting Broadcast, an online service that is part of Office 365. Skype Meeting Broadcast enables users to host and broadcast meetings to large online audiences of up to 10,000 participants. The use of Skype Meeting Broadcast requires that Skype for Business Server already be configured in a hybrid setup with a production Office 365 tenant. All users must have an online tenant established as a prerequisite. If you are interested in deploying a hybrid solution that can take advantage of Skype Meeting Broadcast, see [Configure your on-premises deployment for Skype Meeting Broadcast](#).

## Determine your organizations needs

When you are determining which conferencing capabilities to deploy, you need to consider the features that you want available to your users and your network bandwidth capabilities. The following list guides you through the conferencing planning process to determine what features of conferencing you should deploy, based on your organization's requirements.

### NOTE

When you enable conferencing at deployment, you automatically enable both web and A/V conferencing. You can, however, disable specific features by configuring conferencing policies as described previously in this topic.

- **Do you want to enable web conferencing, which includes document collaboration and application sharing?**

If so, you must enable conferencing for your Front End pool by using the Planning Tool or by using Topology Builder. For more information, see [Deploy conferencing in Skype for Business Server](#).

Application sharing requires and uses more network bandwidth than document collaboration. Skype for Business Server provides a throttling mechanism to control each application sharing session. By default, this is set to 1.5 KB/second for each session. If you do not want to enable application sharing but you do want document collaboration, you can enable conferencing and use conferencing policies to disable application sharing. For details about configuring conferencing policies, see [Manage conferencing policies in Skype for Business Server](#).

To enable users to share PowerPoint presentations, you need to configure Office Web Apps Server. For details about configuring Office Web Apps Server, see [Configure integration with Office Web Apps Server in Skype for Business Server](#).

- **Do you want to enable audio and video conferencing?**

If so, you must enable conferencing for your Front End pool by using the Planning Tool or by using Topology Builder. For more information, see [Deploy conferencing in Skype for Business Server](#).

Audio and video conferencing requires and uses more network bandwidth than web conferencing (which includes document collaboration and application sharing). If you do not want to enable audio and video conferencing but you do want to enable web conferencing, you can enable conferencing and use conferencing policies to disable A/V conferences.

If you do want to enable audio conferences but not video conferences, you can enable A/V conferencing and use conferencing policies to prevent video conferences. Alternatively, you can enable A/V conferencing and enable only certain users to start or participate in A/V conferences.

For more information about configuring conferencing policies, see [Manage conferencing policies in Skype for Business Server](#).

**NOTE**

Enterprise Voice is not required for you to use A/V conferencing. If you enable A/V conferencing, your users can add audio to their conferences if they have audio devices, even if you use a PBX for your telephone solution.

- **Do you want to enable users to join the audio portion of conferences when using a PSTN phone?**

If so, deploy and enable dial-in conferencing. Invited users, both inside and outside your organization, can then join the audio portion of conferences by using a PSTN phone.

Dial-in conferencing is an optional feature that you can configure when you deploy Skype for Business Server conferencing. Although dial-in conferencing uses some of the same components that Enterprise Voice uses, you can deploy dial-in conferencing even if you do not deploy Enterprise Voice. Dial-in conferencing supports both enterprise and anonymous users. For more information about configuring dial-in conferencing for enterprise and anonymous users, see [Deploy conferencing in Skype for Business Server](#) and [Configure dial-in conferencing in Skype for Business Server](#).

- **Do you want to enable external users with Skype for Business clients to join conferences?**

By allowing external participation in meetings, you maximize your investment in Skype for Business Server. External users can include:

- **Remote users.** Your organization's own users, when they are working outside your firewalls and are using their laptops or other Skype for Business Server devices.
- **Federated Users.** Users from companies you work with who also run Skype for Business Server. To enable your users to easily contact these users, you create federated relationships with these

companies.

- **Anonymous Users.** Any other external users who are invited specifically by your users to join specific conferences. A meeting organizer in your company can send an email invitation for a conference to an external user. The email includes a link that the outside user can click to join the conference.

If you want to allow external users, you'll need to deploy Edge Servers. Additionally, with Edge Servers deployed you can create federated relationships with other organizations--such as your customers or vendors--and users from those organizations can more easily collaborate with your users.

For details about deploying Edge Servers, see [Plan for Edge Servers and Deploy Edge Servers](#). For details about enabling external access for Office Web Apps Server, see [Configure integration with Office Web Apps Server in Skype for Business Server](#).

- **Do you want to control the clients that can join Skype for Business Server meetings?**

If so, you should configure the meeting join page so that only the client options that you want to support are available. Each time a user clicks a link to join a scheduled meeting, Skype for Business Server detects whether a client is already installed on the computer. It then starts the default client and opens the meeting join page, which contains links for alternate clients. The meeting join page always contains the option to use Skype for Business Web App. In addition to this option, you can decide whether to include links for Attendee and previous versions of Communicator.



# Hardware and software requirements for conferencing in Skype for Business Server









5/20/2019 • 9 minutes to read

**Summary:** Read this topic to learn about hardware and software requirements for conferencing in Skype for Business Server.

This section describes the hardware and software requirements for web conferencing, audio and video (A/V) conferencing, dial-in conferencing, and instant messaging (IM) conferencing. All conferencing capabilities run on Front End Servers; there are additional requirements for different types of conferencing, as shown in the following diagram.

For example, if you want to allow dial-in conferencing, you'll need to deploy a Mediation Server and a gateway for connecting to the public switched telephone network (PSTN). If you want to allow web conferencing, you'll need to ensure Skype for Business Server can connect to an Office Web Apps Server. If you want to allow external users to participate in conferences, you'll need to deploy an Edge Server.

## Conferencing capabilities and requirements

	Conferencing capabilities	Web conferencing requirements	Dial-in conferencing requirements	External access requirements
<b>Servers</b>	 <b>Front End Server</b>	 <b>Office Web Apps Server</b>	 <b>Mediation Server</b>	 <b>Edge Server</b>
<b>Conferencing capabilities</b>	<b>Instant Messaging</b> <b>Web</b> <b>Audio/Video</b> <b>Dial-in</b>		 <b>PSTN gateway</b>	 <b>Reverse proxy server</b>
<b>Apps and services</b>	<b>Application service</b>	 <b>File share</b>	<b>Attendant app</b> <b>Announcement app</b>	
<b>Network security</b>				<b>Firewall</b> 

For more information about topology considerations, see [Plan your conferencing topology for Skype for Business Server](#).

## Hardware and software requirements for Front End Servers

Because web conferencing, A/V conferencing, dial-in conferencing, and IM conferencing are all collocated with the Front End Server, the server hardware and software requirements are the same as for the Front End Servers. For details about these requirements, see [Server requirements for Skype for Business Server 2015](#) and [Environmental requirements for Skype for Business Server 2015](#) or [Server requirements for Skype for Business Server 2019](#).

## Requirements for web conferencing

If you have chosen to enable web conferencing, you need to plan for the following:

- Access to the file store, which is used for storing web conferencing content.
- Integration with Office Web Apps Server, which is necessary in order to share PowerPoint files during a conference.

### File Store

The Skype for Business Server web conferencing service stores content shared during meetings in the file store. As part of deployment, you must specify a file share to be used as the file store for the Standard Edition server or Enterprise Edition Front End pool. You can use an existing file share for the file store, or you can specify a new file share by specifying the fully qualified domain name (FQDN) of the file server on which the file share is to be located and a folder name for the new file share. For more information, see [Create a file share in Skype for Business Server](#). The web conferencing service encrypts the content before it stores the content in the file store.

Skype for Business Server supports using file shares on either direct attached storage (DAS) or a storage area network (SAN), including Distributed File System (DFS), and on a redundant array of independent disks (RAID) for file stores. After the Skype for Business Server Deployment Wizard has defined the location of the file share, Skype for Business Server creates a folder structure within the file share similar to:

- 1-ApplicationServer-1
- 1-CentralMgmt-1
- 1-WebServices-1
  - CollabContent
  - CollabMetadata
  - DataConf

The web conferencing service then stores content such as PowerPoint slides, whiteboards, polls, and attachments in the CollabContent and CollabMetadata folders, located in the WebServices folder.

### Office Web Apps Server

In order to use web conferencing capabilities, you must install Office Web Apps Server and configure Skype for Business Server to communicate with Office Web Apps Server.

Office Web Apps Server should be installed on a stand-alone computer that is not running Skype for Business Server, SQL Server, or any other server application. (You must not have any version of Office installed on that computer.) Any computer used to run Office Web Apps Server must also have a specific set of software installed (including .NET Framework 4.5 and Windows PowerShell 3.0). These requirements, along with information about configuring certificates and Internet Information Services (IIS), are discussed in detail in the [Microsoft Office Web Apps Deployment website](#).

For information about how to configure Skype for Business Server to work with Office Web Apps Server, see [Configure integration with Office Web Apps Server in Skype for Business Server](#).

## Requirements for audio and video conferencing

To plan for A/V conferencing, you need to understand the network bandwidth required by the type of conferencing media that your organization requires. This could include audio, video, and panoramic video. Without sufficient network bandwidth, the user experience may be severely degraded.

For information about audio and video capacity planning for conferences, see [Plan network requirements for Skype for Business](#).

You can use call admission control (CAC) to manage the network bandwidth used by A/V conferencing. This is important for restricted networks, such as limited bandwidth links between central and branch sites. For details, see [Plan for call admission control in Skype for Business Server](#).

If you deploy audio conferencing in your network, your users will need audio devices such as headsets to participate in an audio conference. If you deploy video conferencing, you need to deploy video devices, such as webcams for users. For both audio and video devices, device deployment and user training are important steps for you to consider. For more information, see [Plan for clients and devices](#). Microsoft recommends that you use unified communications (UC) devices that are certified by Microsoft for all device types, to ensure an optimal user experience. For details about UC-certified devices, see [Phones and devices for Skype for Business](#).

## Requirements for dial-in conferencing

Dial-in conferencing is an optional feature of the Skype for Business Server conferencing workload that includes a variety of components. Some of the components are specific to dial-in conferencing and some are Enterprise Voice components. This section describes the requirements for the components that are needed for dial-in conferencing. For details about Mediation Server and public switched telephone network (PSTN) gateway requirements, see [Mediation Server component in Skype for Business Server](#) and [Deploy a Mediation Server in Topology Builder in Skype for Business Server](#).

### Required components

You will need to install the following Skype for Business Server components before you can configure dial-in conferencing:

- Unified Communications Application Service (UCAS) (called the Application service)
- Conferencing Attendant application
- Conferencing Announcement application
- Dial-in Conferencing Settings webpage
- At least one Mediation Server and at least one PSTN gateway

For dial-in conferencing, Application service, Conferencing Attendant application, and Conferencing Announcement application have the same operating system requirements as Front End Servers. For details, see [Server requirements for Skype for Business Server 2015](#).

Conferencing Attendant application and Conferencing Announcement application require that Windows Media Format Runtime is installed on Front End Servers. Windows Media Format Runtime is required to play Windows Media audio (WMA) files that are used for music on hold, recorded names, and prompts. If you are installing on Windows Server 2012 or Windows Server 2012 R2 (which we recommend), you'll need to install Microsoft Media Foundation to get Windows Media Format Runtime. If you are installing on any version of Windows Server prior to Windows 2012, you need to make sure the Windows Desktop Experience is installed to get Windows Media Format Runtime.

## Audio file requirements for dial-in conferencing

Skype for Business Server does not support customization of voice prompts and music for dial-in conferencing. However, if you have a strong business need that requires you to change the default audio files, see Microsoft Knowledge Base article 961177, [How to customize voice prompts or music files for dial-in audio conferencing](#).

You can also use the [Microsoft Lync Server Conferencing Attendant Custom Voice Prompts](#) management utility, which enables administrators to replace the default voice prompts used when a phone caller joins a Skype for Business meeting with custom prompts to provide a different meeting entry experience. The custom voice prompts can be installed on either an Enterprise or Standard Edition server.

Conferencing Attendant application and Conferencing Announcement application have the following requirements for music on hold, recorded name, and audio prompt files:

- Windows Media Audio (WMA) file format
- 16-bit mono
- 48 kbps 2-pass CBR (constant bit rate)
- Speech level at -24DB

## User requirements for dial-in conferencing

Dial-in conferencing users must have a unique phone number or extension assigned to their account. This requirement supports authentication during dial-in conferencing. Enterprise users (that is, users who have Active Directory Domain Services credentials and Skype for Business Server accounts within your organization) enter their phone number (or extension) and a personal identification number (PIN) to dial in to conferences as an authenticated user.

## Port requirements for conferencing

In order to use the conferencing features, Skype for Business Server requires that certain ports are open. The following table lists port requirements for conferencing. For details about all port requirements, see [Port and protocol requirements for servers](#).

### Required server ports

SERVER ROLE	SERVICE NAME	PORT	PROTOCOL	NOTES
Front End Servers	Skype for Business Server IM Conferencing service	5062	TCP	Used for incoming SIP requests for instant messaging (IM) conferencing.
Front End Servers	Skype for Business Server Web Conferencing service	8057	TCP (TLS)	Used to listen for Persistent Shared Object Model (PSOM) connections from client.
Front End Servers	Skype for Business Server Web Conferencing Compatibility service	8058	TCP (TLS)	Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Skype for Business Server.

<b>SERVER ROLE</b>	<b>SERVICE NAME</b>	<b>PORT</b>	<b>PROTOCOL</b>	<b>NOTES</b>
Front End Servers	Skype for Business Server Audio/Video Conferencing service	5063	TCP	Used for incoming SIP requests for audio/video (A/V) conferencing.
Front End Servers	Skype for Business Server Audio/Video Conferencing service	57501-65535	TCP/UDP	Media port range used for video conferencing.
Front End Servers	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	5064	TCP	Used for incoming SIP requests for dial-in conferencing.
Front End Servers	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	5072	TCP	Used for incoming SIP requests for Attendant (dial in conferencing).
Front End Servers	Skype for Business Server Application Sharing service	5065	TCP	Used for incoming SIP listening requests for application sharing.
Front End Servers	Skype for Business Server Application Sharing service	49152-65535	TCP	Media port range used for application sharing.
Front End Servers	Skype for Business Server Conferencing Announcement service	5073	TCP	Used for incoming SIP requests for the Skype for Business Server Conferencing Announcement service (that is, for dial-in conferencing).
All internal servers	Various	49152-57500	TCP/UDP	Media port range used for audio conferencing on all internal servers. Used by all servers that terminate audio: Front End Servers (for Skype for Business Server Conferencing Attendant service, Skype for Business Server Conferencing Announcement service, and Skype for Business Server Audio/Video Conferencing service), and Mediation Server.
Office Web Apps Servers		443		Used by Skype for Business Server to connect to Office Web Apps Server.

## Required client ports

PORT	PROTOCOL	NOTES
443	TCP (PSOM/TLS)	Used for external user access to web conferencing sessions.
443	TCP (STUN/MSTURN)	Used for external user access to A/V sessions and media (TCP)
3478	UDP (STUN/MSTURN)	Used for external user access to A/V sessions and media (UDP)
1024-65535 *	TCP/UDP	Audio port range (minimum of 20 ports required)
1024-65535 *	TCP/UDP	Video port range (minimum of 20 ports required).
1024-65535 *	TCP	Application sharing.

# Plan your conferencing topology for Skype for Business Server

5/20/2019 • 7 minutes to read

**Summary:** Read this topic to learn about planning your conferencing topology in Skype for Business Server.

This topic describes topology basics for conferencing in Skype for Business Server:

- Supported topologies
- Dial-in conferencing considerations
- Web conferencing considerations
- Requirements for large meetings

For more information about hardware and software requirements, see [Hardware and software requirements for conferencing in Skype for Business Server](#).

## Supported topologies

In Skype for Business Server, the server running conferencing services is always collocated with the Front End Servers or Standard Edition servers. When you deploy Skype for Business Server, IM conferencing capabilities are automatically deployed. You can specify whether to deploy web, audio and video (A/V), and dial-in conferencing by using the Topology Builder. You can also use Topology Builder to add conferencing to an existing deployment. For details about topology basics and collocation scenarios, see [Topology Basics for Skype for Business Server](#).

You can deploy conferencing in the following topologies and configurations:

- Skype for Business Server Standard Edition
- Skype for Business Server Enterprise Edition
- With or without Enterprise Voice

## Dial-in conferencing considerations

If you are deploying dial-in conferencing, you must consider the following:

- Dial-in conferencing requires a Mediation Server to translate signaling (and media in some configurations) between Skype for Business Server and the PSTN gateway, and a PSTN gateway to translate signaling and media between the Mediation Server and the PSTN gateway.

Before you can configure dial-in conferencing, you need to deploy either Enterprise Voice or a Mediation Server and at least one of the following:

- PSTN gateway
  - IP-PBX
  - Session Border Controller (SBC) (for an Internet telephony service provider to which you connect by configuring a SIP trunk)
- You can deploy the Application service, Conferencing Attendant application, and Conferencing Announcement application in a central site, but not in a branch site.

- You must deploy dial-in conferencing in every pool where you deploy Skype for Business Server conferencing. You do not need to assign access numbers in every pool, but you must deploy the dial-in conferencing feature in every pool. This requirement supports the recorded name feature when a user calls an access number from one pool to join a Skype for Business Server conference in a different pool.

For more information, see [Plan for dial-in conferencing in Skype for Business Server](#).

## Web conferencing considerations

Web conferencing requires the following:

- Access to the file store, which is used for storing web conferencing content.
- Integration with Office Web Apps Server/Office Online Server, which is necessary in order to share PowerPoint files during a conference.

### NOTE

The latest iteration of Office Web Apps Server is named Office Online Server, which is supported by Skype for Business Server. For more detail, refer to the [Office Online Server documentation](#).

Skype for Business Server provides the following ways to configure Office Web Apps Server/Office Online Server. Depending on your needs you can:

- **Install both Skype for Business Server and Office Web Apps Server/Office Online Server on-premises behind your organization's firewall, and in the same network zone.** With this topology, external access to Office Web Apps Server/Office Online Server will be provided through your reverse proxy server. Ideally, you should install Office Web Apps Server/Office Online Server in the same network zone as Skype for Business Server.

External Skype for Business clients can connect to Skype for Business Server and to Office Web Apps Server/Office Online Server by using a reverse proxy server, which is a server that takes requests from the Internet and forwards them to the internal network. (Internal clients do not need to use the reverse proxy server because they can connect to Office Web Apps Server/Office Online Server directly.) This topology works best if you want to use a dedicated Office Web Apps Server/Office Online Server farm that is only used by Skype for Business Server.

- **Use an externally deployed Office Web Apps Server/Office Online Server.** In this topology, Skype for Business Server is deployed on-premises, and uses an Office Web Apps Server/Office Online Server that is deployed outside of the Skype for Business Server network zone. This may happen when Office Web Apps Server/Office Online Server is shared across multiple applications in the corporation and is deployed in a network requiring Skype for Business Server to use the external interface of Office Web Apps Server/Office Online Server and vice versa.

You do not need to install a reverse proxy server; instead, all the requests from the Office Web Apps Server/Office Online Server to Skype for Business Server are routed through your Edge Server. Both your internal and your external Skype for Business clients connect to Office Web Apps Server/Office Online Server using the external URL.

If the Office Web Apps Server/Office Online Server is deployed outside your internal firewall, then select the option **Office Web Apps Server is deployed in an external network** (that is, perimeter/Internet) in Topology Builder.

For more information, see [Configure integration with Office Web Apps Server in Skype for Business Server](#).

Regardless of the topology you select, it is critical that the correct firewall ports be opened. You must make sure



that DNS names, IP addresses, and ports are not blocked by firewalls on the Office Web Apps Server/Office Online Server, the load balancer, or Skype for Business Server.

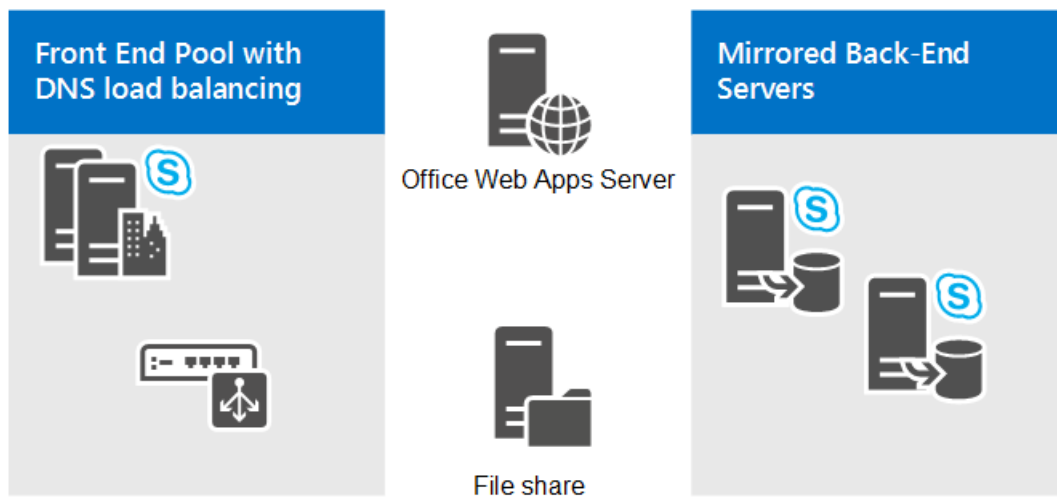
#### NOTE

Another option for providing external access to Office Web Apps Server/Office Online Server is to deploy the server in the perimeter network. If you elect to do this, keep in mind that Office Web Apps Server/Office Online Server setup requires the server computer to be a member of your Active Directory domain. Unless your network policy allows computers in the perimeter network to be Active Directory domain members, it is recommended that you do not install Office Web Apps Server/Office Online Server in the perimeter network. Instead, you should install Office Web Apps Server/Office Online Server in the internal network and provide external user access through your reverse proxy server.

## Topology requirements for large meetings

A single large meeting requires at least one Front End Server and one Back End Server. However, to provide high availability, we recommend a two Front End Server pool with mirrored Back End Servers as shown in the following diagram:

### Large meeting topology



The user who hosts the large meetings must have their user account homed in Front End pool. However, we do not recommend that you host other user accounts in this pool. Instead, use it only for the large meetings. The best practice is to create a special user account in this pool to be used only to host large meetings. Since the large meeting setting is optimized for performance, using it as a normal user could have problems such as the inability to promote a P2P session to a meeting when a PSTN endpoint is involved.

Managing a pool with exactly two Front End Servers requires some special considerations. For more information, see [Topology Basics for Skype for Business Server 2015](#) and [Reference topologies for Skype for Business Server 2015](#).

Additionally, if you want to optionally provide disaster recovery backup and failover for the pool used for large meetings, you can pair it with a similarly set up dedicated pool in a different data center. For details, see [Plan for high availability and disaster recovery in Skype for Business Server](#).

Additional notes about the topology include:

- A file share is required for storing meeting content and, if Archiving Server is deployed and enabled, for storing the archiving files. The file share can be dedicated to the pool or can be the same file share used by another pool at the site in which the pool is deployed. For details about configuring the file share, see [Create a file share in Skype for Business Server 2015](#).
- An Office Web Apps Server/Office Online Server is required for enabling the PowerPoint presentation

functionality in large meetings. The Office Web Apps Server/Office Online Server can be dedicated to the large meeting pool or, it can be the same Office Web Apps Server/Office Online Server used by other pools at the site in which the dedicated pool is deployed. For more information, see [Configure integration with Office Web Apps Server in Skype for Business Server](#).

- Load balancing of the Front End Servers requires hardware load balancing for the HTTP traffic (such as meeting content download). DNS load balancing is recommended for SIP traffic. For details see [Load balancing requirements for Skype for Business](#).
- If you want to use Monitoring Server for the dedicated large-meeting pool, we recommend using the Monitoring Server and its database that are shared across all of the Front End Server pools in your Skype for Business Server deployment. For more information, see [Plan for monitoring in Skype for Business Server](#).

# Plan for dial-in conferencing in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Read this topic to learn about planning for dial-in conferencing in Skype for Business Server.

Dial-in conferencing is an optional feature of Skype for Business Server that allows meeting attendees to join the audio portion of a meeting by calling in to the meeting from a phone. Dial-in conferencing is a subset of audio conferencing and requires additional configuration. This topic describes what you need to think about before deploying dial-in conferencing for your organization.

Some of the components required for dial-in conferencing are specific to dial-in conferencing and some are Enterprise Voice components. Although dial-in conferencing uses some of the same components that Enterprise Voice uses, you can deploy dial-in conferencing even if you do not deploy Enterprise Voice. This section describes the components that are needed for dial-in conferencing. For more information about planning a complete Enterprise Voice solution, see [Plan your Enterprise Voice solution in Skype for Business Server](#).

Dial-in conferencing requires that you provide connectivity to the public switched telephone network (PSTN) by deploying a Mediation Server. In addition to deploying a Mediation Server, you need to consider the following to allow dial-in conferencing for your organization:

- Your plan for connecting to the public switched telephone network (PSTN)
- Your plan for dial plans, access numbers, and conferencing regions
- Your plan for creating conferencing directories
- Your conferencing policy for allowing dial-in access
- Support for enterprise and anonymous users

## NOTE

If you deploy dial-in conferencing, you must deploy it in every pool where you deploy Skype for Business Server conferencing. You do not need to assign access numbers--the numbers participants call to join a conference--in every pool, but you must deploy the dial-in feature in every pool. This requirement supports the recorded name feature when a user calls an access number from one pool to join a Skype for Business Server conference in a different pool.

## Plan for PSTN connectivity

Dial-in conferencing requires at least one Mediation Server and at least one public switched telephone network (PSTN) gateway.

You can deploy a Mediation Server in a central site or in a branch site. In a central site, you can collocate a Mediation Server on a Front End pool or Standard Edition server, or you can deploy it on a stand-alone server or pool. In a branch site, you can deploy a Mediation Server on a stand-alone server or as a component of the Survivable Branch Appliance.

You can deploy a PSTN gateway in a central site or in a branch site. In a branch site, the PSTN gateway can be stand-alone or a component of the Survivable Branch Appliance.

For details about Mediation Server and PSTN gateway requirements, see [Mediation Server component in Skype](#)

for Business Server, [Deploy a Mediation Server in Topology Builder in Skype for Business Server](#), and [Define a gateway in Topology Builder in Skype for Business Server](#).

## Plan for dial plans, access numbers, and conferencing regions

To configure dial-in conferencing, you create dial plans and dial-in conferencing access numbers. You also specify the dial-in regions that associate a dial-in conferencing access number with its dial plans. More specifically:

- Dial plans are sets of normalization rules that specify the number and pattern of digits in a phone number, and translate the phone number into the standard E.164 format required for call routing.
- Dial-in conferencing access numbers are the numbers participants call to join a conference.
- Every dial-in conferencing access number must be associated with at least one dial plan.
- Every dial plan is associated with a conferencing region.

When you create a dial plan, you specify the dial-in conferencing region that applies to the dial plan. When you create the dial-in access number, you select the regions that associate the access number with the appropriate dial plans.

You also specify the scope of the dial plan: user scope, pool scope, or site scope. Every user is assigned the dial plan from the narrowest scope that applies to the user. For example, a user is assigned a user-level dial plan, if one applies. If a user-level dial plan does not apply, the user is assigned a pool-level dial plan. If a pool-level dial plan does not apply, the user is assigned a site-level dial plan. If a site-level dial plan does not apply, the user is assigned the global dial plan.

Before you configure the dial plans, it is important to plan how you want to name and use regions. The following considerations apply to dial-in conferencing regions:

- A region is typically a geographical area that is associated with an office or group of offices.
- Languages are associated with dial-in access numbers. If you support geographical areas that have multiple languages, you should decide how you want to define regions to support the multiple languages. For example, you might define multiple regions based on a combination of geography and language, or you might define a single region based on geography and have different dial-in access numbers for each language.
- When a user schedules a meeting, by default the meeting uses the region specified by that user's dial plan.
- By default, all of the dial-in access numbers for the region are included in the meeting invitation.
- It is important to name regions so that they are clearly recognizable. The user can use the names of the regions to change a meeting's region so that different access numbers are included in the invitation. (When users use Outlook to schedule a meeting, the user uses the Online Meeting Add-in for Skype for Business to change the region).
- Regions should be designed so that any invitee who wants to dial into a conference can see a local access number in the conference invitation.
- You can configure the order in which access numbers within a region appear on the Dial-in Conferencing Settings page (and, therefore, the order in which they appear in the conference invitation) by using Skype for Business Server Management Shell cmdlets.
- Any user from any location can call any dial-in access number to join a conference.

For more information about creating a dial plan, see [Create or modify a dial plan in Skype for Business Server](#) and [Create or modify a normalization rule in Skype for Business](#).

# Plan for conference directories

Conference directories maintain a mapping between the alphanumeric meeting ID that a participant uses to join a conference when using Skype for Business, and the numeric-only conference ID that a dial-in conferencing participant uses to join the conference. The format of the conference ID is as follows:

```
<housekeeping digit (1 digit)><conference directory (usually 1-2 digits)><conference number (variable number of digits)><check digit (1 digit)>
```

Creating multiple conference directories will ensure that conference IDs will stay short until a significant amount of conferences have been created. In an organization with a typical number of conferences per user, we recommend that you create one conference directory for every 999 users in the pool. Using this guideline, the conference IDs can generally be kept small. However, once the number of conference directories (across the pools) exceed 9, the Conference ID number will grow to support additional conferences.

## Plan for a conferencing policy that allows dial-in access

Conferences must be enabled for dial-in access when you configure conferencing policies. By default, conferences that are enabled for dial-in access include the following information in the conference invitation:

- A numeric conference ID that identifies the conference
- One or more PSTN access numbers
- A link to a Dial-in Conferencing Settings page, which contains a complete list of access numbers with their associated languages; a place to create, reset, or unblock personal identification numbers (PINs); and other information, such as dual-tone multi-frequency (DTMF) controls

For more information about conferencing policies, see [Configure dial-in conferencing in Skype for Business Server](#) and [Manage conferencing policies in Skype for Business Server](#).

## Support for enterprise and anonymous users

Dial-in conferencing supports both enterprise and anonymous users. Enterprise users have Active Directory Domain Services credentials and Skype for Business Server accounts within their organization. Anonymous users do not have enterprise credentials within your organization. In the dial-in conferencing context, a user in a federated partner's organization who uses the PSTN to connect to a conference is treated like an anonymous user. For dial-in conferencing, unlike other contexts, federated users are not authenticated.

Enterprise users or conference leaders who join a conference that is enabled for dial-in access dial one of the conference access numbers and then are prompted to enter the conference ID. If a leader has not yet joined the meeting, users can either enter their unified communications (UC) extension (or full phone number) and PIN or wait to be admitted by a leader. The Meeting organizer can join the meeting as a leader by entering just their PIN. The Front End Server uses the combination of full phone number or extension, and PIN, to uniquely map enterprise users to their Active Directory credentials. As a result, enterprise users are authenticated and identified by name in the conference. Enterprise users can also assume a conference role predefined by the organizer.

### NOTE

Enterprise users who dial in from an office IP phone or from Skype for Business Server Attendant are not prompted for their phone number because they are already authenticated.

Anonymous users who want to join a dial-in conference dial one of the conference access numbers and then they are prompted to enter the conference ID. Unauthenticated anonymous users are also prompted to record their

name. The recorded name identifies unauthenticated users in the conference. Anonymous users are not admitted to the conference until at least one leader or authenticated user has joined, and they cannot be assigned a predefined role.

**NOTE**

Enterprise users who choose not to enter their phone number and PIN are not authenticated. They are prompted to record their name and are treated as anonymous users in the conference.

When scheduling a meeting, the meeting organizer can choose to restrict access to the meeting by making the meeting closed or locked. In this case, dial-in users are requested to authenticate.

- If dial-in users fail or choose not to authenticate, they are transferred to the lobby where they wait until a leader accepts or rejects them, or they time out and are disconnected.
- After they are admitted to a conference, dial-in users can participate in the audio portion of the conference and can exercise dual-tone multi-frequency (DTMF) commands by using the phone keypad.
- Dial-in leaders can exercise DTMF commands to turn participants' ability to unmute on or off, lock or unlock the conference, admit people from the lobby, and turn entry and exit announcements on or off.
- Leaders can also use a DTMF command to admit everyone from the lobby, which changes the permissions of the meeting to allow anyone who subsequently joins.
- All dial-in participants can exercise DTMF commands to hear Help, listen to the conference roster, and mute themselves.
- Dial-in participants (that is, whether or not they dial from the PSTN) hear personal announcements during the conference, such as whether they have been muted or unmuted, whether the meeting is being recorded, or whether someone is waiting in the lobby.

**NOTE**

Participants who join the conference by clicking a link instead of dialing in do not hear personal announcements.

# Plan for large meetings in Skype for Business Server

6/4/2019 • 12 minutes to read

**Summary:** Read this topic to learn about best practices for implementing and managing large meetings in Skype for Business Server.

The size of meetings that Skype for Business Server can support depends on whether conferencing is hosted on a shared or dedicated pool: anywhere from 250 participants on a shared pool to 1000 participants on a dedicated pool.

## NOTE

This topic focuses on best practices for large meetings supported by Skype for Business Server. If your organization requires larger meeting capabilities, you should consider implementing a hybrid environment that takes advantage of Skype Meeting Broadcast, a new online service that is part of Office 365.

## NOTE

Skype Meeting Broadcast enables users to host and broadcast meetings to large online audiences of up to 10,000 participants. The use of Skype Meeting Broadcast requires that Skype for Business Server already be configured in a hybrid setup with a production Office 365 tenant. All users must have an online tenant established as a prerequisite. If you are interested in deploying a hybrid solution that can take advantage of Skype Meeting Broadcast, see [What is a Skype Meeting Broadcast?](#) and [Configure your on-premises deployment for Skype Meeting Broadcast](#).

Large meetings typically have the following characteristics:

- The meeting format is a one-to-many presentation.
- One or a few users are presenters, and everyone else participates only as attendees.
- PowerPoint presentation sharing is the main data collaboration activity.
- Audio is required and video may also be used.
- A dedicated person, generally either the meeting organizer or an assistant to the organizer, sets up the meeting well in advance.
- Dedicated staff (not the presenters) runs the meeting, including connecting to an online meeting, verifying that audio, video, and slide sharing work, managing lobby and user roles, muting and unmuting participants, taking questions, and managing recordings, as appropriate.

When a user schedules a meeting, Skype for Business Server creates a record in the conferencing database, which stores conferencing data, but does not reserve any hardware resources for the scheduled meeting ahead of time. Instead, Skype for Business Server has built-in load balancing logic to dynamically allocate conferencing resources on Front End Servers in a way that distributes loads equally across all Front End Servers in the pool. This effectively provisions and uses hardware resources, but it is important that you plan appropriately to support very large meetings.

For example, when a Skype for Business Server pool is running close to its top capacity, each Front End Server might host approximately 125 average-size meetings. Adding another small meeting would not be a problem, but adding a meeting for 1000 users would be a problem because the Front End Servers would probably not be able to support such a large meeting at the same time as the other 125 meetings.

Supporting large meetings of up to 1000 participants requires addressing the issues related to both the shared hardware model and the no-reservation model. In general, you need to plan for a dedicated pool and follow best practices as described in the following sections.

## Plan for a dedicated pool

If your organization requires meetings with greater than 250 participants, you need to plan for a dedicated pool to support the load.

To have sufficient CPU and memory resources for meetings of up to 1000 users, the hosting Front End Servers should not host any other instant messaging (IM) and presence or Enterprise Voice workloads. The servers should also not host any other meetings, regardless of the size of the other meetings. To host meetings of up to 1000 users, you need to set up a separate Skype for Business Server pool that is dedicated to hosting large meetings.

A Skype for Business Server pool that is dedicated to hosting large meetings should host one and only one meeting of up to 1000 users at the same time, so meeting times need to be reserved in advance via an out of band scheduling process to ensure dedicated support from the Front End Servers. To support more than one large meeting at the same time, you should set up multiple dedicated large-meeting pools.

For more information about hardware and software requirements, and planning a topology that supports large meetings, see [Hardware and software requirements for conferencing in Skype for Business Server](#) and [Plan your conferencing topology for Skype for Business Server](#).

## Implement best practices for large meetings

After setting up a dedicated pool for large meetings, you can take steps to help ensure that large meetings hosted in the pool provide the best user experience. The following sections provide guidelines for managing large meetings:

- Create dedicated meeting organizers
- Create dedicated moderators
- Maintain a separate calendar of large meetings
- Implement a large-meeting scheduling process
- Specify appropriate scheduling details
- Create a conferencing policy for large meetings

### **Create dedicated meeting organizers**

To minimize the real-time communications traffic in the large-meeting pool, Microsoft does not recommend hosting users who regularly sign in using Skype for Business clients and participate in instant messaging (IM), presence, conferencing, and voice sessions. Instead, do one of the following:

- Create one or more dedicated user accounts just for scheduling large meetings
- Home the user accounts of the staff responsible for scheduling large meetings on a large-meeting pool

### **Create dedicated moderators**

With several hundred to a thousand users in a meeting, it is a good practice to have a dedicated person moderate the online session of a large meeting. This dedicated person can be a delegate of the meeting organizer or a member of the organization's large-meeting support staff. It is important to add the dedicated meeting moderator as a presenter at the time that the meeting is scheduled, although it is possible to promote an online meeting attendee to the presenter role while the meeting is in progress.

The meeting moderator can use all presenter functionalities of Skype for Business clients to manage the large



meeting. These functionalities include:

- Monitoring the lobby and admitting or rejecting users in the lobby
- Removing any users from the meeting who should not be in the meeting
- Changing meeting access types
- Changing participant roles
- Inviting additional participants during the meeting using drag and drop functionality, phone dial out, or email
- Muting and unmuting the audience or individual users
- Managing meeting content, including uploading content, deleting content, and switching active content

### **Maintain a separate calendar**

For each large-meeting pool, you should maintain a separate calendar of large meetings scheduled on that pool. For example, you can have a single user account on the large-meeting pool and use Outlook with Exchange and Online Meeting Add-in for Skype for Business to maintain a separate calendar. If you use multiple user accounts to enable a support staff to create large meetings, you can set up a separate calendar that aggregates all large meetings created by the members of the support staff.

Maintaining a separate large meeting calendar helps to prevent conflicts and ensure that only one large meeting is active at any time.

### **Implement a scheduling process**

Because only one large meeting at a time is supported on the dedicated large meeting pool, you should implement a large meeting scheduling process to facilitate setting up large meetings and help prevent conflicts. Such capability is not provided directly by Skype for Business Server or Skype for Business clients. One way to implement such a process is to use your organization's support team's ticketing system, if available.

Scheduling a large meeting involves completing the following steps:

- The meeting organizer or delegate determines the time, duration, and size of an upcoming meeting, in addition to the list of presenters. If the anticipated meeting size exceeds 250 users or to ensure the best user experience for a meeting of fewer than 250 users, the organizer or the delegate submits a request for a large meeting.
- The scheduling staff checks to see whether the requested date and time is available. Since we support only a single large meeting on the dedicated pool at a time, the scheduling staff needs to check the large-meeting calendar to determine whether there is another meeting scheduled for the requested date and time. If the requested time is available, the staff approves the meeting request.
- If the request is approved, the scheduling staff (using credentials on the dedicated pool) uses Online Meeting Add-in for Skype for Business with Outlook to set up a meeting on the dedicated large-meeting pool. The URL to be used to join the meeting is provided to the requester as part of the approval notice.
- The meeting organizer or delegate uses Outlook to schedule the upcoming meeting, adding the URL for joining the meeting to the meeting invitation. The meeting organizer or delegate then specifies the users to be invited and sends out the meeting invitation.

### **Specify appropriate scheduling details**

After checking to ensure that no other meeting is scheduled at the requested time, the large meeting support staff that handles the request schedules the meeting on the large-meeting pool.

To ensure the best user experience, it is important to schedule the large meeting with the right access levels and meeting settings that are appropriate to the meeting organizer's needs. Consider the following scheduling settings

configured in Skype for Business Meeting options:

- Use a new meeting space for each large meeting instead of reusing the dedicated meeting space.
- Specify the meeting access level as follows:
  - If at least one invitee is external to the organization, set the meeting access type to **Anyone (no restrictions)**. This enables you to avoid having to manage a potentially large lobby when the meeting is in progress.
  - If the meeting is an internal-only meeting, set the meeting access type to **Anyone from my organization**.

**NOTE**

Avoid setting the meeting access type to **People I invite from my company** because when you use this setting, organizers must add all user email addresses to the invitee list and you cannot invite a distribution group. Avoid setting the meeting access type to **Only me, the meeting organizer** because this setting requires that every meeting participant, including presenters, must be put in the lobby at meeting run time. The person responsible for running the large meeting must then constantly monitor the lobby roster and admit new users who are in the lobby.

- Allow users who dial-in from phones to enter the meeting automatically by checking the **Callers get in directly** setting.
- Explicitly invite the following users:
  - Meeting organizer and delegate (requester)
  - The list of presenters provided by a meeting requester

**NOTE**

If the meeting access type is set to **People I choose**, you need to explicitly add each participant of a large meeting as an invitee of the meeting.

- Explicitly manage presenters, instead of setting the presenter option to one of the auto-promote values. Be sure to add the following users as presenters:
  - Meeting organizer and delegate (requester)
  - The list of presenters provided by large meeting requesters

By explicitly managing presenters, you can limit presenters to a small enough number to make it possible to have an effective large meeting. If the majority of meeting participants have the attendee role, it helps reduce the chance of people accidentally taking control of the presentation, deleting a PowerPoint presentation, muting/unmuting presenters, and other disruptions to the meeting.

- Check the **Mute all attendees** setting to make sure that only presenters can broadcast audio into the meeting.
- Check the **Block attendees' video** setting to make sure only presenters can broadcast video into the meeting.

### Create a conferencing policy

Create a new conferencing policy specifically for large meetings, and then assign the conferencing policy to the users who are homed on the dedicated large-meeting pool. Configure the conferencing policy using the following settings:

- Set the **MaxMeetingSize** option to 1000. (The default is 250.)
- Set the **AllowLargeMeetings** option to **True**.
- Set the **EnableAppDesktopSharing** option to **None**.
- Set the **AllowUserToScheduleMeetingsWithAppSharing** option to **False**.
- Set the **AllowSharedNotes** option to **False**.
- Set the **AllowAnnotations** option to **False**.
- Set the **DisablePowerPointAnnotations** option to **True**.
- Set the **AllowMultiview** option to **False**.
- Set the **EnableMultiviewJoin** option to **False**.

#### NOTE

Support for large meetings in Skype for Business Server requires that the **AllowLargeMeetings** setting be set to true. When this setting is set to true, the Skype for Business experience will be optimized for extra-large meetings when users join the meeting. Specifically, in a large meeting, Skype for Business will not show the initial or update of the full meeting participant list, which is a performance bottleneck for both the client and Skype for Business Server. Instead, Skype for Business will only show information about the user and the list of presenters of the meeting. Skype for Business will still show the total number of participants available in the large meetings.

The **AllowLargeMeetings \$true** setting causes the following:

- Hides the Attendee roster.
- Disables errors in the IM window.
- Disables multi-party video.
- Disables ability to promote an Attendee to Presenter. You must plan ahead and declare all Presenters before the meeting.
- Disables ability to unmute individual Attendees.
- Disables ability to apply the Lock Video Spotlight feature to Attendees.
- PSTN dial in users will be unable to unmute themselves using 6 because Personal Virtual Assistance which is responsible for DTMF commands in active large meetings is missing.
- If the presenter/organizer schedules a meeting where everyone should be muted first ("Mute All"), PSTN users will be muted throughout the call and will not be able to unmute themselves.

Except for the **Maximum meeting size** setting, all the other conferencing policy settings specified here are required in order to disable conferencing capabilities that are not necessary in large meetings.

Additionally, you need to configure the dedicated large-meeting pool so that each Skype for Business Server user who is homed on the pool and responsible for managing the meeting schedule has the appropriate permissions. To do this, do the following:

- Set the **Designate as presenter** option to **None**. Typically, one or just a few users of all the participants of a large meeting are presenters, so participants should not be automatically admitted to large meetings as presenters. Instead, the presenters should be explicitly designated at meeting scheduling time, or be explicitly promoted during the large meeting.
- Make sure that the **Assigned conference type by default** check box is not selected. This setting controls

whether the Online Meeting Add-in for Skype for Business always schedules conferences using the organizer's assigned conference, which means that scheduled meetings have the same join URL and audio information. In small group collaboration scenarios, having such assigned conference type works well because everyone has their own individual assigned conference, and the constant join URL and audio information helps to facilitate faster meeting joining. However, in the large-meeting scenario, the large meeting support staff schedules the large meetings using a single set of user credentials, and then provides join URLs and audio information to the meeting requesters. In this case, using a different URL to join each meeting works better.

- Ensure that the **Admit anonymous users by default** check box is not selected, unless it is required. This setting affects the default meeting access type scheduled by the Online Meeting Add-in for Skype for Business when not using an assigned conference. The appropriate option for this setting depends on your organization's needs. If most large meetings for your organization are internal meetings, do not select this option. If most large meetings require that external users be able to join, select this option.

For more information about creating a conferencing policy, see [Manage conferencing policies in Skype for Business Server](#).

# Plan for Edge Server deployments in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Plan for your Skype for Business Server Edge environment. This topic introduces you to Edge concepts and lets you get organized with our more in-depth topics.

When you have a Skype for Business Server environment that's working well internally, the next step for you might be to introduce an Edge Server or an Edge pool to the environment. This role would be vital if you want the services provided by Skype for Business Server to be used by people who are outside your internal network. These can potentially include:

- Remote Users: Employees who are offsite, either temporarily or in an ongoing way.
- Federated Users: Your partner organizations' employees.
- Mobile Users.
- Potential customers, partners and even anonymous users you want to invite to meetings and presentations.

External User Access, which is what Edge Servers provide, allow all this to happen. Your internal users will be able to enjoy the following services that are hosted by your Skype for Business Server deployment:

- IM and presence for communication: Authorized external users can join in IM conversations and conferences. They can get presence information for other users (who get their presence info too). You won't be able to do multiparty conferences if you're using a public IM provider, that's strictly peer-to-peer communication. But both SIP and XMPP protocols are supported.
- Audio/video (A/V) conferencing: Authorized external users can participate in your Skype for Business Server audio and video conferences.
- Web conferencing: Your authorized external users can participate in your Skype for Business conferences. You can also enable participation for remote users, federated users, and anonymous users if you'd like. Public IM users can't participate in conferences. There are also options to let these users participate in application and desktop sharing, and even act as meeting organizers or presenters.

Mobile device access is supported, as is Enterprise Voice. You can invite external users to those meetings you wish them to attend, even anonymous users, if you want to give permissions to them.

If this sounds like something your organization needs, then planning for an Edge environment's going to be a big help in deploying it. For further reading, we have the topics listed below.

## NOTE

XMPP Gateways and proxies are available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See [Migrating XMPP federation](#) for more information.

## Planning topics:

The planning articles are:

- [Edge Server system requirements in Skype for Business Server 2015](#)

- [Edge Server environmental requirements in Skype for Business Server 2015](#)
- [Edge Server scenarios in Skype for Business Server 2015](#)

# Edge Server system requirements in Skype for Business Server

5/20/2019 • 10 minutes to read

**Summary:** Learn about the system requirements for Edge Server in Skype for Business Server.

When it comes to your Skype for Business Server Edge Server deployment, these are the things you'll need to do for the server or servers that are in the environment itself, as well as planning for the environment structure. For more information on topology, DNS, certificates, and other infrastructure concerns, check out the environmental requirements documentation.

## Components

When discussing the Edge Server environment, we're referencing components that are, for the most part, deployed in a perimeter network (that's to say it's either in a workgroup or a domain that's outside your Skype for Business Server domain structure).

Keeping that in mind, these are the components you're going to need to keep in mind for deploying your Edge successfully:

- [Edge Servers](#)
- [Reverse proxies](#)
- [Firewalls](#)
- [Directors](#) (these are optional, and if they're included, they'll be located on your internal network)
- [Load Balancers](#) (you can have DNS load balancing or a hardware load balancer (HLB), but for a single Edge Server, this isn't needed)

We have more detail on each of these below:

### Edge Servers

These are the Skype for Business servers deployed in your perimeter environment. Their role is to send and receive network traffic to external users for the services offered by your internal Skype for Business Server deployment. To do this successfully, each Edge Server runs:

- **Access Edge service:** Provides a single, trusted connection point for both outbound and inbound Session Initiation Protocol (SIP) traffic.
- **Web Conferencing Edge service:** Enables external users to join meetings that are hosted on your internal Skype for Business Server environment.
- **A/V Edge service:** Makes audio, video, application sharing and file transfer available to external users.
- **XMPP Proxy service:** Accepts and sends extensible messaging and presence protocol (XMPP) messages to and from configured XMPP Federated partners.

Authorized external users can use your Edge Servers to connect to your internal Skype for Business Server deployment, but otherwise, they provide no other access to your internal network for anyone.

#### NOTE

Edge Servers are deployed to provide connections for enabled Skype for Business clients and other Edge Servers (in federation scenarios). You can't connect from other end point client or server types. The XMPP Gateway server can allow connections with configured XMPP partners. But again, those are the only client and federation types that will work.

#### NOTE

XMPP Gateways and proxies are available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See [Migrating XMPP federation](#) for more information.

### Reverse proxies

A reverse proxy (RP) server has no Skype for Business Server role, but is an essential component of an Edge Server deployment. A reverse proxy allows external users to:

- connect to meetings or dial-in conferences using simple URLs.
- download meeting content.
- expand distribution groups.
- get user-based certificates for client certificate based authentication
- download files from the Address Book Server, or to submit queries to the Address Book Web Query service.
- obtain updates to client and device software.

And for mobile devices:

- it lets them automatically discover Front End Servers offering mobility services.
- it enables push notifications from Office 365 to mobile devices.

Our current reverse proxy recommendations can be found on the [Telephony Infrastructure for Skype for Business](#) page. So your reverse proxy:

- should be able to use transport layer security (TLS) that's introduced to your environment via public certificates to connect to the published external Web services of:
  - Director or Director pool
  - Front End Server or Front End pool
- needs to be able to publish internal Web sites using certificates for encryption, or publish them over an unencrypted means, if needed.
- should be able to publish an internally hosted web site externally by using a fully qualified domain name (FQDN).
- needs to be able to publish all the contents of your hosted web site. By default, you can use the `/^*` directive, which is recognized by most web servers to mean "Publish all content on the web server." You can also modify the directive—for example, `/Uwca/^*`, which means "Publish all content under the virtual directory Uwca."
- must require TLS connections with clients that request content from your published website.
- has to accept certificates with subject alternative name (SAN) entries.



- needs to be able to allow the binding of a certificate to a listener or interface through which the external web services FQDN will resolve. Listener configurations are preferable to interfaces. Many listeners can be configured on a single interface.
- must allow for the configuration of host header handling. Often, the original host header sent by the requesting client must be passed transparently, instead of being modified by the reverse proxy.
- should allow bridging of TLS traffic from one externally defined port (for example, TCP 443) to another defined port (for example, TCP 4443). Your reverse proxy may decrypt the packet on receipt and then reencrypt the packet on sending.
- should allow bridging of unencrypted TCP traffic from one port (for example, TCP 80) to another (for example, TCP 8080).
- needs to allow configuration of, or accept, NTLM authentication, no authentication, and pass-through authentication.

If your reverse proxy can address all the needs in this list, you should be good to go, but please keep in mind our recommendations at the link provided above.

### Firewalls

You need to put your Edge deployment behind an external firewall, but we recommend having two firewalls, one external, and one internal between the Edge environment and your internal environment. All our documentation in our Scenarios will have two firewalls. We recommend two firewalls because it ensures strict routing from one network edge to the other, and doubles the firewall protection for your internal network.

### Directors

This is an optional role. It can be a single server or a pool of servers running the Director role. It's a role found on the internal Skype for Business Server environment.

The Director is an internal next hop server which receives inbound SIP traffic from the Edge Servers that's destined for Skype for Business Server internal servers. It preauthenticates inbound requests and redirects them to a user's home pool or server. This preauthentication allows you to drop unidentified user account requests.

Why does that matter? An important function for a Director is to protect Standard Edition servers and Front End Servers or Front End pools from malicious traffic, such as denial-of-service (DoS) attacks. If your network is flooded with invalid external traffic, the traffic stops at the Director.

### Load Balancers

The Skype for Business Server scaled consolidated Edge topology is optimized for DNS load balancing for new deployments, and we recommend this. If you need high availability, we recommend using a hardware load balancer for one specific situation:

- Exchange UM for remote users using Exchange UM **prior** to Exchange 2013.

#### IMPORTANT

It's vital to note that you can't mix load-balancers. In your Skype for Business Server environment all interfaces must use either DNS or HLB.

#### NOTE

Direct server return (DSR) NAT isn't supported for Skype for Business Server.

For any Edge Server running the A/V Edge service, these are the requirements:

- Turn off TCP nagling for both internal and external ports 443 (nagling is the process of combining several small packets into a single, larger packet for more efficient transmission).
- Turn off TCP nagling for the external port range 50000 - 59999.
- Don't use NAT on your internal or external firewalls.
- Your Edge internal interface must be on a different network than your Edge Server external interface, and routing between them must be disabled.
- The external interface of any Edge Server running the A/V Edge service must use publicly routable IP addresses and no NAT or port translation on any of the Edge external IP addresses.

#### HLB requirements

Skype for Business Server doesn't have a lot of cookie-based affinity requirements. So you don't need to use a cookie-based persistence **unless** (and this is Skype for Business Server 2015-specific) you're going to have Lync Server 2010 Front End Servers or Front End pools in your Skype for Business Server environment. They would need cookie-based affinity in the configuration method recommended for Lync Server 2010.

#### NOTE

If you decide to turn cookie-based affinity on for your HLB, there won't be a problem doing so, even if your environment doesn't need it.

If your environment **doesn't** need cookie-based affinity:

- On the reverse proxy publishing rule for port 443, set **Forward host header** to **True**. This will ensure the original URL is forwarded.

For deployments that **do** need cookie-based affinity:

- On the reverse proxy publishing rule for port 443, set **Forward host header** to **True**. This will ensure the original URL is forwarded.
- The hardware load balancer cookie **must not** be marked httpOnly.
- The hardware load balancer cookie **must not** have an expiration time.
- The hardware load balancer cookie **must** be named **MS-WSMAN** (this is the value that the Web services expect, and it can't be changed).
- The hardware load balancer cookie **must** be set in every HTTP response for which the incoming HTTP request didn't have a cookie, regardless of whether a previous HTTP response on that same TCP connection had gotten a cookie. If your hardware load balancer optimizes cookie insert to only occur once per TCP connection, that optimization **must not** be used.

#### NOTE

It's typical for HLB configurations to use source-affinity and 20 minute TCP session lifetime, which is fine for Skype for Business Server and its clients, because session state is maintained through client usage, and/or application interaction.

If you're deploying mobile devices, your HLB must be able to load balance individual requests within a TCP session (in effect, you need to be able to load balance an individual request based on the target IP address).

## IMPORTANT

F5 HLBs have a feature called OneConnect. It ensures that each request within a TCP connection is individually load balanced. If you're deploying mobile devices, ensure your HLB vendor supports the same functionality. The latest iOS mobile apps require TLS version 1.2. If you need to know more, F5 provides specific settings for this.

Here are the HLB requirements for the (optional) Director and (required) Front End pool Web Services:

- For your internal Web Services VIPs, set Source\_addr persistence (internal port 80, 443) on your HLB. For Skype for Business Server, Source\_addr persistence means that multiple connections coming from a single IP address are always sent to one server, to maintain session state.
- Use a TCP idle timeout of 1800 seconds.
- On the firewall between your reverse proxy and your next hop pool's HLB, create a rule to allow https: traffic on port 4443, from your reverse proxy to your HLB. Your HLB needs to be configured to listen on ports 80, 443, and 4443.

### Summary of HLB affinity requirements

CLIENT/USER LOCATION	EXTERNAL WEB SERVICES FQDN AFFINITY REQUIREMENTS	INTERNAL WEB SERVICES FQSN AFFINITY REQUIREMENTS
Skype for Business Web App (internal and external users) Mobile device (internal and external users)	No affinity	Source address affinity
Skype for Business Web App (external users only) Mobile device (internal and external users)	No affinity	Source address affinity
Skype for Business Web App (internal users only) Mobile device (not deployed)	No affinity	Source address affinity

### Port monitoring for HLBs

You define port monitoring on your hardware load balancers to determine when specific services are no longer available, due to hardware or communications failure. For example, if the Front End Server service (RTCSRVR) stops because the Front End Server or Front End pool fails, the HLB monitoring should also stop receiving traffic on the Web Services. You should implement port monitoring on the HLB to monitor the following for your HLB external interface:

VIRTUAL IP/PORT	NODE PORT	NODE MACHINE/MONITOR	PERSISTENCE PROFILE	NOTES
<pool>web_mco_443_vs_443	4443	Front End 5061	None	HTTPS
<pool>web_mco_80_vs_80	8080	Front End 5061	None	HTTP

## Hardware and software requirements

We've covered Edge Server hardware and software requirements in our overall [Server requirements for Skype for Business Server 2015](#) and [System requirements for Skype for Business Server 2019](#) documentation.

## Collocation

We've covered Edge Server collocation in our [Topology Basics for Skype for Business Server](#) documentation.

# Edge Server environmental requirements in Skype for Business Server

7/1/2019 • 30 minutes to read

**Summary:** Learn about the environmental requirements for Edge Server in Skype for Business Server.

A lot of planning and preparation needs to take place outside of the Skype for Business Server Edge Server environment itself. In this article, we'll review what preparations need to be made in the organizational environment, as per our list below:

- [Topology planning](#)
- [DNS planning](#)
- [Certificate planning](#)
- [Port and firewall planning](#)

## Topology planning

Skype for Business Server Edge Server topologies are able to use:

- Routable public IP addresses.
- Non-routable private IP addresses, if **symmetric** network address translation (NAT) is used.

### TIP

Your Edge Server can be configured to use a single IP address with distinct ports for each service, or it can use distinct IP addresses for each service, but use the same default port (which by default will be TCP 443). We have more information in IP Address requirements section, below.

If you choose non-routable private IP addresses with NAT, remember these points:

- You need to use routable private IP addresses on **all three** external interfaces.
- You need to configure **symmetric** NAT for incoming and outgoing traffic. Symmetric NAT is the only supported NAT you can use with Skype for Business Server Edge Server.
- Configure your NAT to not change incoming source addresses. The A/V Edge service needs to be able to receive the incoming source address to find the optimal media path.
- Your Edge Servers need to be able to communicate with one another from their public A/V Edge IP addresses. Your firewall needs to allow this traffic.
- NAT can **only** be used for scaled consolidated Edge Servers if you use DNS load balancing. If you use hardware load balancing (HLB), you need to use publicly routable IP addresses **without** NAT.

You'll have no problems having your Access, Web conferencing and A/V Edge interfaces behind a router or firewall performing symmetric NAT for both single and scaled consolidated Edge Server topologies (as long as you're not using hardware load balancing).

### Summary of Edge Server topology options

We have several topology options available for Skype for Business Server Edge Server deployments:

- Single consolidated Edge with private IP addresses and NAT
- Single consolidated Edge with public IP addresses
- Scaled consolidated Edge with private IP addresses and NAT
- Scaled consolidated Edge with public IP addresses
- Scaled consolidated Edge with hardware load balancers

To help you choose one, we have the following table which gives a summary of what options you have for each topology:

TOPOLOGY	HIGH AVAILABILITY	ADDITIONAL DNS RECORDS REQUIRED FOR EXTERNAL EDGE SERVER IN THE EDGE POOL?	EDGE FAILOVER FOR SKYPE FOR BUSINESS SERVER SESSIONS	EDGE FAILOVER FOR SKYPE FOR BUSINESS SERVER FEDERATION SESSIONS
Single consolidated Edge with private IP addresses and NAT	No	No	No	No
Single consolidated Edge with public IP addresses	No	No	No	No
Scaled consolidated Edge with private IP addresses and NAT (DNS load balanced)	Yes	Yes	Yes	Yes <sup>1</sup>
Scaled consolidated Edge with public IP addresses (DNS load balanced)	Yes	Yes	Yes	Yes <sup>1</sup>
Scaled consolidated Edge with hardware load balancers	Yes	No (one DNS A record per VIP)	Yes	Yes

<sup>1</sup> Exchange Unified Messaging (UM) remote user failover using DNS load balancing requires Exchange 2013 or newer.

### IP Address requirements

On a fundamental level, three services need IP addresses; Access Edge service, Web Conferencing Edge service, and A/V Edge service. You have the option of either using three IP addresses, one for each of the services, or you can use one and opt to put each service on a different port (you can check out the [Port and firewall planning](#) section for more information on some of that). For a single consolidated Edge environment, that's pretty much it.

#### NOTE

As noted above, you can choose to have one IP address for all three services and run them on different ports. But to be clear, we don't recommend this. If your customers can't access the alternate ports you'd be using in this scenario, they can't access the full functionality of your Edge environment, either.

It can be a little more complicated with scaled consolidated topologies, so let's look at some tables that lay out the IP Address requirements, keeping in mind that the primary decision points for topology selection are high

availability and load balancing. High availability needs can influence your load balancing choice (we'll talk about that more after the tables).

**IP Address requirements for scaled consolidated Edge (IP Address per role)**

NUMBER OF EDGE SERVERS PER POOL	NUMBER OF REQUIRED IP ADDRESSES FOR DNS LOAD BALANCING	NUMBER OF REQUIRED IP ADDRESSES FOR HARDWARE LOAD BALANCING
2	6	3 (1 per VIP) + 6
3	9	3 (1 per VIP) + 9
4	12	3 (1 per VIP) + 12
5	15	3 (1 per VIP) + 15

**IP Address requirements for scale consolidated Edge (Single IP address for all roles)**

NUMBER OF EDGE SERVERS PER POOL	NUMBER OF REQUIRED IP ADDRESSES FOR DNS LOAD BALANCING	NUMBER OF REQUIRED IP ADDRESSES FOR HARDWARE LOAD BALANCING
2	2	1 (1 per VIP) + 2
3	3	1 (1 per VIP) + 3
4	4	1 (1 per VIP) + 4
5	5	1 (1 per VIP) + 5

Let's look at some additional things to think about while planning.

- **High availability:** If you need high availability in your deployment, you should deploy at least two Edge Servers in a pool. It's worth noting that a single Edge pool will support up to 12 Edge Servers (though Topology Builder will allow you to add up to 20, that's not tested or supported, so we advise you don't do that). If you need more than 12 Edge Servers, you should create additional Edge pools for them.
- **Hardware load balancing:** We recommend DNS load balancing for most scenarios. Hardware load balancing is also supported, of course, but notably it's required for a single scenario over DNS load balancing:
  - External access to Exchange 2007 or Exchange 2010 (with no SP) Unified Messaging (UM).
- **DNS load balancing:** For UM, Exchange 2010 SP1 and newer are able to be supported by DNS load balancing. Note that if you need to go with DNS load balancing for an earlier version of Exchange, it'll work, but all the traffic for this will go to the first server in the pool, and if it's not available, that traffic will subsequently fail.

DNS load balancing is also recommended if you're federating with companies using:

- Skype for Business Server 2015:
  - Lync Server 2010
  - Lync Server 2013
  - Microsoft Office O365
- Skype for Business Server 2019:
  - Lync Server 2013
  - Skype for Business Server 2015

- Microsoft Office 365.

## DNS planning

When it comes to Skype for Business Server Edge Server deployment, it's vital to prepare for DNS properly. With the right records in place, the deployment will be much more straightforward. Hopefully you've chosen a topology in the section above, as we're going to do an overview, and then list a couple of tables outlining the DNS records for those scenarios. We'll also have some [Advanced Edge Server DNS planning for Skype for Business Server](#) for more in-depth reading, if you need it.

### DNS records for Single consolidated Edge Server scenarios

These will be the DNS records you're going to need for a single Edge Server using either public IPs or private IPs with NAT. Because this is sample data, we'll give example IPs so you can work out your own entries more easily:

- Internal network adapter: 172.25.33.10 (no default gateways assigned)

#### NOTE

Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Skype for Business Server or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).

- External network adapter:
  - Public IPs:
    - Access Edge: 131.107.155.10 (this is the primary, with default gateway set to your public router, ex: 131.107.155.1)
    - Web Conferencing Edge: 131.107.155.20 (secondary)
    - A/V Edge: 131.107.155.30 (secondary)

Web conferencing and A/V Edge public IP addresses are additional (secondary) IP addresses in the Advanced section of the properties of Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) of the Local Area Connection Properties in Windows Server.

- Private IPs:
  - Access Edge: 10.45.16.10 (this is the primary, with default gateway set to your router, ex: 10.45.16.1)
  - Web Conferencing Edge: 10.45.16.20 (secondary)
  - A/V Edge: 10.45.16.30 (secondary)

Web conferencing and A/V Edge public IP addresses are additional (secondary) IP addresses in the Advanced section of the properties of Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) of the Local Area Connection Properties in Windows Server.

#### TIP

There are other possible configurations here:

- You could use one IP address on the external network adapter. We don't recommend this because then you're going to need to differentiate between the three services using different ports (which you can do in Skype for Business Server) but there are some firewalls that may block the alternate ports. See the [Port and firewall planning](#) section for more about this.



- You can have three external network adapters instead of one, and assign one of the service IPs to each one. Why do this? It would separate the services and if something goes wrong, that would make it easier to troubleshoot, and potentially let your other services continue working while you resolve an issue.

LOCATION	TYPE	PORT	FQDN OR DNS RECORD	IP ADDRESS OR FQDN	NOTES
External DNS	A record	NA	sip.contoso.com	<b>public:</b> 131.107.155.10 <b>private:</b> 10.45.16.10	An external interface for your Access Edge service. You'll need one for every SIP domain with Skype for Business users.
External DNS	A record	NA	webcon.contoso.com	<b>public:</b> 131.107.155.20 <b>private:</b> 10.45.16.20	An external interface for your Web Conferencing Edge service.
External DNS	A record	NA	av.contoso.com	<b>public:</b> 131.107.155.30 <b>private:</b> 10.45.16.30	An external interface for your A/V Edge service.
External DNS	SRV record	443	_sip._tls.contoso.com	sip.contoso.com	An external interface for your Access Edge service. This SRV record is required for Skype for Business Server, Lync Server 2013, and Lync Server 2010 clients to work externally. You'll need one for every domain with Skype for Business users.
External DNS	SRV record	5061	_sipfederationtls._tcp.contoso.com	sip.contoso.com	An external interface for your Access Edge service. This SRV record is required for automatic DNS discovery of federated partners called Allowed SIP domains. You'll need one for every domain with Skype for Business users.

LOCATION	TYPE	PORT	FQDN OR DNS RECORD	IP ADDRESS OR FQDN	NOTES
Internal DNS	A record	NA	sfvedge.contoso.net	172.25.33.10	The internal interface for your consolidated Edge.

### DNS records for Scaled DNS and hardware Edge Server scenarios

These will be the DNS records you're going to need for a single Edge Server using either public IPs or private IPs with NAT. Because this is sample data, we'll give example IPs so you can work out your own entries more easily:

- Internal network adapter:
  - Node 1: 172.25.33.10 (no default gateway's assigned)
  - Node 2: 172.25.33.11 (no default gateway's assigned)

#### NOTE

Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Skype for Business Server or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).

- External network adapter:
  - Node 1
    - Public IPs:
      - Access Edge: 131.107.155.10 (this is the primary, with default gateway set to your public router, ex: 131.107.155.1)
      - Web Conferencing Edge: 131.107.155.20 (secondary)
      - A/V Edge: 131.107.155.30 (secondary)

Web conferencing and A/V Edge public IP addresses are additional (secondary) IP addresses in the Advanced section of the properties of Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) of the Local Area Connection Properties in Windows Server.
    - Private IPs:
      - Access Edge: 10.45.16.10 (this is the primary, with default gateway set to your router, ex: 10.45.16.1)
      - Web Conferencing Edge: 10.45.16.20 (secondary)
      - A/V Edge: 10.45.16.30 (secondary)

Web conferencing and A/V Edge public IP addresses are additional (secondary) IP addresses in the Advanced section of the properties of Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) of the Local Area Connection Properties in Windows Server.

- Node 2
  - Public IPs:

- o Access Edge: 131.107.155.11 (this is the primary, with default gateway set to your public router, ex: 131.107.155.1)
- o Web Conferencing Edge: 131.107.155.21 (secondary)
- o A/V Edge: 131.107.155.31 (secondary)

Web conferencing and A/V Edge public IP addresses are additional (secondary) IP addresses in the Advanced section of the properties of Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) of the Local Area Connection Properties in Windows Server.

o Private IPs:

- o Access Edge: 10.45.16.11 (this is the primary, with default gateway set to your router, ex: 10.45.16.1)
- o Web Conferencing Edge: 10.45.16.21 (secondary)
- o A/V Edge: 10.45.16.31 (secondary)

Web conferencing and A/V Edge public IP addresses are additional (secondary) IP addresses in the Advanced section of the properties of Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) of the Local Area Connection Properties in Windows Server.

There are other possible configurations here:

- You could use one IP address on the external network adapter. We don't recommend this because then you're going to need to differentiate between the three services using different ports (which you can do in Skype for Business Server) but there are some firewalls that may block the alternate ports. See the [Port and firewall planning](#) section for more about this.
- You can have three external network adapters instead of one, and assign one of the service IPs to each one. Why do this? It would separate the services and if something goes wrong, that would make it easier to troubleshoot, and potentially let your other services continue working while you resolve an issue.

LOCATION	TYPE	PORT	FQDN OR DNS RECORD	IP ADDRESS OR FQDN	NOTES
External DNS	A record	NA	sip.contoso.com	<b>public:</b> 131.107.155.10 and 131.107.155.11 <b>private:</b> 10.45.16.10 and 10.45.16.11	An external interface for your Access Edge service. You'll need one for every SIP domain with Skype for Business users.
External DNS	A record	NA	webcon.contoso.com	<b>public:</b> 131.107.155.20 and 131.107.155.21 <b>private:</b> 10.45.16.20 and 10.45.16.21	An external interface for your Web Conferencing Edge service.

LOCATION	TYPE	PORT	FQDN OR DNS RECORD	IP ADDRESS OR FQDN	NOTES
External DNS	A record	NA	av.contoso.com	<b>public:</b> 131.107.155.30 and 131.107.155.31 <b>private:</b> 10.45.16.30 and 10.45.16.31	An external interface for your A/V Edge service.
External DNS	SRV record	443	_sip._tls.contoso.com	sip.contoso.com	An external interface for your Access Edge service. This SRV record is required for Skype for Business Server, Lync Server 2013, and Lync Server 2010 clients to work externally. You'll need one for every domain with Skype for Business.
External DNS	SRV record	5061	_sipfederationtls._tcp.contoso.com	sip.contoso.com	An external interface for your Access Edge service. This SRV record is required for automatic DNS discovery of federated partners called Allowed SIP domains. You'll need one for every domain with Skype for Business.
Internal DNS	A record	NA	sfvedge.contoso.net	172.25.33.10 and 172.25.33.11	The internal interface for your consolidated Edge.

#### DNS record for federation (all scenarios)

LOCATION	TYPE	PORT	FQDN	FQDN HOST RECORD	NOTES
----------	------	------	------	------------------	-------

LOCATION	TYPE	PORT	FQDN	FQDN HOST RECORD	NOTES
External DNS	SRV	5061	_sipfederationtls_ tcp.contoso.com	sip.contoso.com	<p>The SIP Access Edge external interface required for automatic DNS discovery. Used by your other potential federation partners. It's also known as "Allow SIP domains." You'll need one of these for each SIP domain with Skype for Business users.</p> <p><b>Note:</b> You will need this SRV record for mobility and the push notification clearing house.</p>

#### DNS records for extensible messaging and presence protocol

LOCATION	TYPE	PORT	FQDN	IP ADDRESS OR FQDN HOST RECORD	NOTES
----------	------	------	------	--------------------------------	-------

LOCATION	TYPE	PORT	FQDN	IP ADDRESS OR FQDN HOST RECORD	NOTES
External DNS	SRV	5269	_xmpp-server_tcp.contoso.com	xmpp.contoso.com	The XMPP proxy interface on your Access Edge service or Edge pool. You need to repeat this as needed for all internal SIP domains with Skype for Business Server enabled users, where contact with XMPP contacts is allowed through: <ul style="list-style-type: none"> <li>• a global policy</li> <li>• a site policy where the user's enabled</li> <li>• a user policy applied to the Skype for Business Server enabled user</li> </ul> An allowed XMPP policy also needs to be configured in the XMPP federated users policy.
External DNS	SRV	A	xmpp.contoso.com	IP address of the Access Edge service on the Edge Server or Edge pool hosting your XMPP Proxy service	This points to the Access Edge service on the Edge Server or Edge pool that hosts the XMPP Proxy service. Typically the SRV record that you create will point to this host (A or AAAA) record.

**NOTE**

XMPP Gateways and proxies are available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See [Migrating XMPP federation](#) for more information.

## Certificate planning

Skype for Business Server uses certificates for secure, encrypted communications both between servers and from server to client. As you'd expect, your certificates will need to have DNS records for your servers match up to any subject name (SN) and subject alternate name (SAN) on your certificates. This will take work now, at the planning stage, to ensure you have the right FQDNs registered in DNS for the SN and SAN entries for your certificates.

We'll discuss external and internal certificate needs separately, and then look at a table providing the requirements for both.

## External Certificates

At a minimum, the certificate assigned to your external Edge Server interfaces will need to be provided by a public Certificate Authority (CA). We can't recommend a specific CA to you, but we do have a list of CAs, [Unified Communications certificate partners](#) that you can take a look at to see if your preferred CA is listed.

When will you need to submit a request to a CA for this public certificate, and how do you do it? There are a couple of ways to accomplish this:

- You can go through the installation of Skype for Business Server, and then the Edge Server deployment. The Skype for Business Server Deployment Wizard will have a step to generate a certificate request, which you can then send to your chosen CA.
- You can also use Windows PowerShell commands to generate this request, if that's more inline with your business needs or deployment strategy.
- Finally, your CA may have their own submission process, which may also involve Windows PowerShell or another method. In that case, you'll need to rely on their documentation, in addition to the information provided here for your reference.

After you've gotten the certificate, you'll need to go ahead and assign it to these services in Skype for Business Server:

- Access Edge service interface
- Web Conferencing Edge service interface
- Audio/Video Authentication service (don't confuse this with the A/V Edge service, as that doesn't use a certificate to encrypt audio and video streams)

### IMPORTANT

All Edge Servers (if they belong to the same pool of Edge Servers) need to have the exact same certificate with the same private key for the Media Relay Authentication service.

## Internal Certificates

For the internal Edge Server interface, you can use a public certificate from a public CA, or a certificate issued from your organization's internal CA. The thing to remember about the internal certificate is that it uses an SN entry, and no SAN entries, so you don't have to worry about SAN on the internal cert at all.

### Required Certificates table

We have a table here to help you out with your requests. The FQDN entries here are for sample domains only. You're going to need to make requests based on your own private and public domains, but here's a guide to what we've used:

- contoso.com: Public FQDN
- fabrikam.com: Second public FQDN (added as a demo of what to request if you have multiple SIP domains)
- Contoso.net: Internal domain

### Edge Certificate table

Regardless of whether you're doing a single Edge Server or an Edge pool, this is what you'll need for your certificate:

COMPONENT	SUBJECT NAME (SN)	SUBJECT ALTERNATIVE NAMES (SAN)/ORDER	NOTES
External Edge	sip.contoso.com	sip.contoso.com webcon.contoso.com sip.fabrikam.com	<p>This is the certificate you need to request from a public CA. It'll need to be assigned to the external Edge interfaces for the following:</p> <ul style="list-style-type: none"> <li>• Access Edge</li> <li>• Web Conferencing Edge</li> <li>• Audio/Video Authentication</li> </ul> <p>The good news is that SANs are automatically added to your certificate request, and therefore your certificate after you submit the request, based on what you defined for this deployment in Topology Builder. You'll only need to add SAN entries for any additional SIP domains or other entries you need to support. Why is sip.contoso.com replicated in this instance? That happens automatically as well, and it's needed for things to work properly.</p> <p><b>Note:</b> This certificate can also be used for Public Instant Messaging connectivity. You don't need to do anything differently with it, but in previous versions of this documentation, it was listed as a separate table, and now it's not.</p>
Internal Edge	sfbedge.contoso.com	NA	You can get this certificate from a public CA or an internal CA. It'll need to contain the server EKU (Enhanced Key Usage), and you'll assign it to the internal Edge interface.

If you need a certificate for Extensible Messaging and Presence Protocol (XMPP), it will look identical to the External Edge table entries above, but will have the following two additional SAN entries:

- xmpp.contoso.com
- \*.contoso.com

Please remember that currently XMPP is only supported in Skype for Business Server for Google Talk, if you want or need to use it for anything else, you need to confirm that functionality with the third-party vendor involved.

## Port and firewall planning



Getting your planning right for ports and firewalls for Skype for Business Server Edge Server deployments can save you days or weeks of troubleshooting and stress. As a result, we're going to list a couple of tables that will indicate our protocol usage and what ports you need to have open, inbound and outbound, both for NAT and public IP scenarios. We'll also have separate tables for hardware load balanced scenarios (HLB) and some further guidance on that. For more reading from there, we also have some [Edge Server scenarios in Skype for Business Server](#) you can check out for your particular deployment concerns.

### General protocol usage

Before we look at the summary tables for external and internal firewalls, let's consider the following table as well:

AUDIO/VIDEO TRANSPORT	USAGE
UDP	The preferred transport layer protocol for audio and video.
TCP	The fallback transport layer protocol for audio and video. The required transport layer protocol for application sharing to Skype for Business Server, Lync Server 2013, and Lync Server 2010. The required transport layer protocol for file transfer to Skype for Business Server, Lync Server 2013, and Lync Server 2010.

### External port firewall summary table

The Source IP address and Destination IP address will contain information for users who are using Private IP addresses with NAT, as well as people using public IP addresses. This will cover all the permutations in our [Edge Server scenarios in Skype for Business Server](#) section.

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
XMPP Not supported in Skype for Business Server 2019	TCP	5269	Any	XMPP Proxy service (shares an IP address with the Access Edge service)	The XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations.
Access/HTTP	TCP	80	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Any	Certificate revocation and CRL check and retrieval.
Access/DNS	TCP	53	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Any	DNS query over TCP.

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
Access/DNS	UDP	53	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Any	DNS query over UDP.
Access/SIP(TLS)	TCP	443	Any	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Client-to-server SIP traffic for external user access.
Access/SIP(MTLS)	TCP	5061	Any	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	For federated and public IM connectivity using SIP.
Access/SIP(MTLS)	TCP	5061	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Any	For federated and public IM connectivity using SIP.
Web conferencing/PSOM(TLS)	TCP	443	Any	<b>Private IP using NAT:</b> Edge Server Web Conferencing Edge service <b>Public IP:</b> Edge Server Web Conferencing Edge service public IP address	Web conferencing media.
A/V/RTP	TCP	50000-59999	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	Any	This is used for relaying media traffic.

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
A/V/RTP	UDP	50000-59999	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	Any	This is used for relaying media traffic.
A/V/STUN.MSTURN	UDP	3478	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	Any	3478 outbound is: <ul style="list-style-type: none"> <li>• Used by Skype for Business Server to determine the version of Edge Server it's communicating with.</li> <li>• Used for media traffic between Edge Servers.</li> <li>• Required for federation with Lync Server 2010.</li> <li>• Needed if multiple Edge pools are deployed within your organization.</li> </ul>
A/V/STUN.MSTURN	UDP	3478	Any	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP on port 3478.
A/V/STUN.MSTURN	TCP	443	Any	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP on port 443.
A/V/STUN.MSTURN	TCP	443	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	Any	STUN/TURN negotiation of candidates over TCP on port 443.

**Internal port firewall summary table**

PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
XMPP/MTLS	TCP	23456	Any of the following running the XMPP Gateway service: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Front End pool</li> </ul>	Edge Server internal interface	Outbound XMPP traffic from your XMPP Gateway service running on your Front End Server or Front End pool. <b>Note:</b> XMPP Gateways and proxies are available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See <a href="#">Migrating XMPP federation</a> for more information.
SIP/MTLS	TCP	5061	Any: <ul style="list-style-type: none"> <li>• Director</li> <li>• Director pool</li> <li>• Front End Server</li> <li>• Front End pool</li> </ul>	Edge Server internal interface	Outbound SIP traffic from your Director, Director pool, Front End Server or Front End pool to your Edge Server internal interface.
SIP/MTLS	TCP	5061	Edge Server internal interface	Any: <ul style="list-style-type: none"> <li>• Director</li> <li>• Director pool</li> <li>• Front End Server</li> <li>• Front End pool</li> </ul>	Inbound SIP traffic to your Director, Director pool, Front End Server, or Front End pool from your Edge Server internal interface.
PSOM/MTLS	TCP	8057	Any: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Each Front End Server in your Front End pool</li> </ul>	Edge Server internal interface	Web conferencing traffic from your Front End Server or each Front End Server (if you have a Front End pool) to your Edge Server internal interface.

PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
SIP/MTLS	TCP	5062	Any: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Front End pool</li> <li>• Any Survivable Branch Appliance using this Edge Server</li> <li>• Any Survivable Branch Server using this Edge Server</li> </ul>	Edge Server internal interface	Authentication of A/V users from your Front End Server or Front End pool, or your Survivable Branch Appliance or Survivable Branch Server, using your Edge Server.
STUN/MSTURN	UDP	3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between your internal and external users and your Survivable Branch Appliance or Survivable Branch Server.
STUN/MSTURN	TCP	443	Any	Edge Server internal interface	Fallback path for A/V media transfer between your internal and external users and your Survivable Branch Appliance or Survivable Branch Server, if UDP communication doesn't work. TCP is then used for file transfers and desktop sharing.
HTTPS	TCP	4443	Any: <ul style="list-style-type: none"> <li>• Front End Server that holds the Central Management store</li> <li>• Front End pool that holds the Central Management store</li> </ul>	Edge Server internal interface	Replication of changes from your Central Management store to your Edge Server.

PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
MTLS	TCP	50001	Any	Edge Server internal interface	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe ) or agent (ClsAgent.exe) commands and log collection.
MTLS	TCP	50002	Any	Edge Server internal interface	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe ) or agent (ClsAgent.exe) commands and log collection.
MTLS	TCP	50003	Any	Edge Server internal interface	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe ) or agent (ClsAgent.exe) commands and log collection.

### Hardware load balancers for Edge port tables

We're giving hardware load balancers (HLBs) and Edge ports their own section, as things are a little more complicated with the additional hardware. Please refer to the tables below for guidance for this particular scenario:

#### External port firewall summary table

The Source IP address and Destination IP address will contain information for users who are using Private IP addresses with NAT, as well as people using public IP addresses. This will cover all the permutations in our [Edge Server scenarios in Skype for Business Server](#) section.

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
Access/HTTP	TCP	80	Edge Server Access Edge service public IP address	Any	Certificate revocation and CRL check and retrieval.
Access/DNS	TCP	53	Edge Server Access Edge service public IP address	Any	DNS query over TCP.
Access/DNS	UDP	53	Edge Server Access Edge service public IP address	Any	DNS query over UDP.
A/V/RTP	TCP	50000-59999	Edge Server A/V Edge service IP address	Any	This is used for relaying media traffic.
A/V/RTP	UDP	50000-59999	Edge Server A/V Edge service public IP address	Any	This is used for relaying media traffic.
A/V/STUN.MSTURN	UDP	3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is: <ul style="list-style-type: none"> <li>• Used by Skype for Business Server to determine the version of Edge Server it's communicating with.</li> <li>• Used for media traffic between Edge Servers.</li> <li>• Required for federation.</li> <li>• Needed if multiple Edge pools are deployed within your organization.</li> </ul>
A/V/STUN.MSTURN	UDP	3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP on port 3478.

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
A/V/STUN.MSTURN	TCP	443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP on port 443.
A/V/STUN.MSTURN	TCP	443	Edge Server A/V Edge service public IP address	Any	STUN/TURN negotiation of candidates over TCP on port 443.

**Internal port firewall summary table**

PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
XMPP/MTLS	TCP	23456	Any of the following running the XMPP Gateway service: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Front End pool VIP address running the XMPP Gateway service</li> </ul>	Edge Server internal interface	Outbound XMPP traffic from your XMPP Gateway service running on your Front End Server or Front End pool.  <b>Note:</b> XMPP Gateways and proxies are available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See <a href="#">Migrating XMPP federation</a> for more information.
HTTPS	TCP	4443	Any: <ul style="list-style-type: none"> <li>• Front End Server that holds the Central Management store</li> <li>• Front End pool that holds the Central Management store</li> </ul>	Edge Server internal interface	Replication of changes from your Central Management store to your Edge Server.



PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
PSOM/MTLS	TCP	8057	Any: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Each Front End Server in your Front End pool</li> </ul>	Edge Server internal interface	Web conferencing traffic from your Front End Server or each Front End Server (if you have a Front End pool) to your Edge Server internal interface.
STUN/MSTURN	UDP	3478	Any: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Each Front End Server in your Front End pool</li> </ul>	Edge Server internal interface	Preferred path for A/V media transfer between your internal and external users and your Survivable Branch Appliance or Survivable Branch Server.
STUN/MSTURN	TCP	443	Any: <ul style="list-style-type: none"> <li>• Front End Server</li> <li>• Each Front End Server in your pool</li> </ul>	Edge Server internal interface	Fallback path for A/V media transfer between your internal and external users and your Survivable Branch Appliance or Survivable Branch Server, if UDP communication doesn't work. TCP is then used for file transfers and desktop sharing.
MTLS	TCP	50001	Any	Edge Server internal interface	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe ) or agent (ClsAgent.exe) commands and log collection.

PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
MTLS	TCP	50002	Any	Edge Server internal interface	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection.
MTLS	TCP	50003	Any	Edge Server internal interface	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection.

#### External interface Virtual IPs

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
XMPP Not Supported in Skype for Business Server 2019	TCP	5269	Any	XMPP Proxy service (shares an IP address with the Access Edge service)	The XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations.
XMPP Not Supported in Skype for Business Server 2019	TCP	5269	XMPP Proxy service (shares an IP address with the Access Edge service)	Any	The XMPP Proxy service sends traffic from XMPP contacts in defined XMPP federations.

ROLE OR PROTOCOL	TCP OR UDP	DESTINATION PORT OR PORT RANGE	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
Access/SIP(TLS)	TCP	443	Any	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Client-to-server SIP traffic for external user access.
Access/SIP(MTLS)	TCP	5061	Any	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	For federated and public IM connectivity using SIP.
Access/SIP(MTLS)	TCP	5061	<b>Private IP using NAT:</b> Edge Server Access Edge service <b>Public IP:</b> Edge Server Access Edge service public IP address	Any	For federated and public IM connectivity using SIP.
Web conferencing/PSOM(TLS)	TCP	443	Any	<b>Private IP using NAT:</b> Edge Server Web Conferencing Edge service <b>Public IP:</b> Edge Server Web Conferencing Edge service public IP address	Web conferencing media.
A/V/STUN.MSTURN	UDP	3478	Any	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP on port 3478.
A/V/STUN.MSTURN	TCP	443	Any	<b>Private IP using NAT:</b> Edge Server A/V Edge service <b>Public IP:</b> Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP on port 443.

#### Internal interface Virtual IPs

Our guidance here is going to be a little different. In actuality, in a HLB situation, we now recommend you only have routing through an internal VIP under the following circumstances:

- If you are using Exchange 2007 or Exchange 2010 Unified Messaging (UM).
- If you have legacy clients using the Edge.

The following table does give guidance for those scenarios, but otherwise, you should be able to depend on Central Management store (CMS) to route traffic to the individual Edge Server it's aware of (this does require that CMS is kept up to date on Edge Server information, of course).

PROTOCOL	TCP OR UDP	PORT	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	NOTES
Access/SIP(MTLS)	TCP	5061	Any: <ul style="list-style-type: none"> <li>• Director</li> <li>• Director pool VIP address</li> <li>• Front End Server</li> <li>• Front End pool VIP address</li> </ul>	Edge Server internal interface	Outbound SIP traffic from your Director, Director pool VIP address, Front End Server, or Front End pool VIP address to your Edge Server internal interface.
Access/SIP(MTLS)	TCP	5061	Edge Server internal VIP interface	Any: <ul style="list-style-type: none"> <li>• Director</li> <li>• Director pool VIP address</li> <li>• Front End Server</li> <li>• Front End pool VIP address</li> </ul>	Inbound SIP traffic to your Director, Director pool VIP address, Front End Server, or Front End pool VIP address from your Edge Server internal interface.
SIP/MTLS	TCP	5062	Any: <ul style="list-style-type: none"> <li>• Front End Server IP address</li> <li>• Front End pool IP address</li> <li>• Any Survivable Branch Appliance using this Edge Server</li> <li>• Any Survivable Branch Server using this Edge Server</li> </ul>	Edge Server internal interface	Authentication of A/V users from your Front End Server or Front End pool, or your Survivable Branch Appliance or Survivable Branch Server, using your Edge Server.
STUN/MSTURN	UDP	3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between your internal and external users.

<b>PROTOCOL</b>	<b>TCP OR UDP</b>	<b>PORT</b>	<b>SOURCE IP ADDRESS</b>	<b>DESTINATION IP ADDRESS</b>	<b>NOTES</b>
STUN/MSTURN	TCP	443	Any	Edge Server internal VIP interface	Fallback path for A/V media transfer between your internal and external users if UDP communication doesn't work. TCP is then used for file transfers and desktop sharing.

# Advanced Edge Server DNS planning for Skype for Business Server

7/17/2019 • 12 minutes to read

**Summary:** Review scenarios for Skype for Business Server deployment options. Whether you want a single server or prefer a server pool with DNS or HLB, this topic should help.

When it comes to Domain Name System (DNS) planning for Skype for Business Server, there are a lot of factors that may play into your decision. If your organization's domain structure's already in place, this may be a matter of reviewing how you're going to proceed. We'll begin with the topics found below:

- [Walkthrough of Skype for Business clients locating services](#)
- [Split-brain DNS](#)
- [Automatic configuration without split-brain DNS](#)
- [DNS disaster recovery](#)
- [DNS load balancing](#)

## Walkthrough of Skype for Business clients locating services

Skype for Business clients are similar to previous versions of Lync clients in how they find and access services in Skype for Business Server. This section details the server location process.

1. `lyncoverinternal.<domain>`

*This is an A host record for the Autodiscover service on the internal web services.*

2. `lyncover.<domain>`

*This is an A host record for the Autodiscover service on the external web services.*

3. `_sipinternaltls._tcp.<domain>`

*This is a SRV record for internal TLS connections.*

4. `_sip._tls.<domain>`

*This is a SRV record for external TLS connections.*

5. `sipinternal.<domain>`

*This is an A host record for the Front End pool or Director, resolvable only on the internal network.*

6. `sip.<domain>`

*This is an A host record for the Front End pool or Director, resolvable only on the internal network.*

7. `sipexternal.<domain>`

*This is an A host record for the Access Edge service, when the client is external.*

The Autodiscover service is always favored as that's the preferred method for service location, and the others are fallback methods.

## NOTE

When you're creating SRV records, it's important to remember that they need to point to a DNS A (and AAAA if you're using IPv6 addressing) in the same domain in which the DNS SRV record's being created. For example, if they SRV record's in contoso.com, the A (and AAAA) record it points to can't be in fabrikam.com.

If you're inclined to do it, you can set your mobile device up for manual discovery of services. If that's what you're looking to do, each user needs to configure their mobile device settings with the full internal and external Autodiscover service URIs, including the protocol and path, as follows:

- For external access: `https://<ExtPoolFQDN>/Autodiscover/autodiscover.service.svc/Root`
- For internal access: `https://<IntPoolFQDN>/AutoDiscover/AutoDiscover.svc/Root`

We do recommend you use automatic discovery as opposed to manual discovery. But if you're doing some troubleshooting or testing, manual settings can be very helpful.

## Split-brain DNS

This is a DNS configuration where you have two DNS zones with the same namespace. The first DNS zone handles internal requests, while the second DNS zone handles external requests.

Why would a company do this? They may have a requirement to use the same namespace internally and externally, but of course this will lead to many DNS SRV and A records being unique to one zone or another, and where there is duplication, the IP addresses associated with these records would be unique.

This presents some challenges. The most important is that split-brain DNS is **not supported** for Mobility. This is because of the LyncDiscover and LyncDiscoverInternal DNS records (LyncDiscover has to be defined on your external DNS server, while LyncDiscoverInternal has to be defined on your internal DNS server).

We'll list the DNS records for the internal and external zones here, but you can find detailed examples on the Edge Server environmental requirements section.

### Internal DNS

- Contains a DNS zone called (for example) contoso.com, for which it's authoritative.
- This internal contoso.com contains:
  - DNS A and AAAA (if you're using IPv6 addressing) records for your Front End pool, Director pool or Director pool name, and all internal servers running Skype for Business Server in your organization's network.
  - DNS A and AAAA (if you're using IPv6 addressing) records for your Edge internal interface for each Skype for Business Server Edge Server in your perimeter network.
  - DNS A and AAAA (if you're using IPv6 addressing) records for the internal interface of each reverse proxy server in your perimeter network (which is **optional** for management of a reverse proxy).
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for internal Skype for Business Server client autoconfiguration (which is **optional**).
  - DNS A and AAAA (if you're using IPv6 addressing) or CNAME records for automatic discovery of Skype for Business Server Web Services (which is **optional**).
- All your Skype for Business Server internal Edge interfaces in your perimeter network use this internal DNS zone for resolving queries to contoso.com.
- All servers running Skype for Business Server, and clients running Skype for Business Server in the

corporate network, point to internal DNS servers for resolving queries to contoso.com, or they use the Host file on each Edge Server and list A and AAAA (if you're using IPv6 addressing) records for the next hop server (specifically for the Director or Director pool VIP, Front End pool VIP, or Standard Edition server).

## External DNS

- Contains a DNS zone called (for example) contoso.com, for which it's authoritative.
- This external contoso.com contains:
  - DNS A and AAAA (if you're using IPv6 addressing), or CNAME records, for automatic discovery of Skype for Business Server web services. This is for use with mobility.
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for the Edge external interface of each Skype for Business Server Edge Server or hardware load balanced (HLB) VIP in the perimeter network.
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for the external interface of the Reverse proxy server or (VIP for a pool of Reverse proxy servers), in the perimeter network.
  - DNS A and AAAA (if you're using IPv6 addressing) and SRV records for Skype for Business Server client autoconfiguration (**optional**).

## Automatic configuration without split-brain DNS

If you don't use split-brain DNS, internal automatic configuration of clients running Skype for Business won't work unless you're using one of the workarounds we have here. Why not? Because Skype for Business Server requires the user's SIP URI to match the domain of the Front End pool designated for automatic configuration. This hasn't changed from earlier versions of Lync Server.

So, if you have two SIP domains in use, you'd need these DNS SRV records:

- `_sipinternaltls._tcp.contoso.com. 86400 IN SRV 0 0 5061 pool01.contoso.com`

*If a user signs in as bob@contoso.com, this record would work for automatic configuration, as the user's SIP domain matches the domain of the Front End pool (contoso.com).*

- `_sipinternaltls._tcp.fabrikam.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com`

*If a user signs in as alice@fabrikam.com, this record would work for automatic configuration of the second domain, again because the SIP domain matches the Front End pool for that domain.*

To take the example further, this would not work:

- `_sipinternaltls._tcp.litwareinc.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com`

*A user signing in as tim@litwareinc.com won't work for automatic configuration, because his SIP domain (litwareinc.com) doesn't match the domain in the pool (fabrikam.com).*

So now that we know all that, if you need automatic requirement for your Skype for Business clients without split-brain DNS, you have these options:

- **Group Policy Objects**

You can use Group Policy Objects (GPOs) to populate the correct server values.

### NOTE

This option doesn't enable automatic configuration, but it does automate manual configuration. If this approach is used, the SRV records associated with automatic configuration aren't required.



- **Matching internal zone**

You'll need to create a zone in your internal DNS that matches your external DNS zone (for example, contoso.com), and then create DNS A (and AAAA if you're using IPv6 addressing) records that correspond to the Skype for Business Server pool used for automatic configuration.

For example, if you have a user homed on pool01.contoso.net, but signs into Skype for Business as bob@contoso.com, create an internal DNS zone called contoso.com, and inside it you need to create a DNS A (and AAAA if IPv6 addressing's being used) record for pool01.contoso.com.

- **Pin-point internal zone**

If creating an entire zone in your internal DNS isn't an option for you, you can create pin-point (dedicated) zones that correspond to the SRV records required for automatic configuration, and populate those zones using dnscmd.exe. Dnscmd.exe is required because the DNS user interface won't support the creation of pin-point zones.

For example, if your SIP domain is contoso.com, and you have a Front End pool called pool01 that contains two Front End Servers, you'll need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.contoso.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.contoso.com. @ SRV 0 0 5061 pool01.contoso.com.
dnscmd . /zoneadd pool01.contoso.com. /dsprimary
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
```

You may have a second SIP domain in your environment. In that case, you'll need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.fabrikam.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.fabrikam.com. @ SRV 0 0 5061 pool01.fabrikam.com.
dnscmd . /zoneadd pool01.fabrikam.com. /dsprimary
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.fabrikam.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.fabrikam.com. @ AAAA <IPv6 address>
```

#### **NOTE**

You'll see the Front End pool FQDN appears twice, but with two different IP addresses. That's because DNS load balancing is used. If HLB is used, there'd only be a single Front End pool entry.

#### **NOTE**

Also, the Front End pool FQDN values change between the contoso.com and fabrikam.com examples, but the IP addresses remain the same. That's because users who're signing in from either SIP domain will be using the same Front End pool for automatic configuration.

## DNS disaster recovery

To configure DNS to redirect Skype for Business Server web traffic to your disaster recover (DR) and failover sites, you need to use a DNS provider that supports GeoDNS. You can set up your DNS records to support disaster recover, so that features that use web services continue even if one entire Front End pool goes down. This DR

feature supports the Autodiscover, Meet and Dial-in simple URLs.

You define and configure additional DNS host A (AAAA if using IPv6) records for internal and external resolution of web services at your GeoDNS provider. The following details assume paired pools, geographically dispersed, and that the GeoDNS supported by your provider **either** has round-robin DNS **or** is configured to use Pool1 as primary and fails over to Pool2 in the event of any communications loss or power failure.

All the DNS records in this table are examples.

GEODNS RECORD	POOL RECORDS	CNAME RECORDS	DNS SETTINGS (SELECT ONE OPTION)
Meet-int.geolb.contoso.com	Pool1 InternalWebFQDN.contoso.com Pool2 InternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1 InternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2 InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Meet-ext.geolb.contoso.com	Pool1 ExternalWebFQDN.contoso.com Pool2 ExternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1 ExternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2 ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Dialin-int.geolb.contoso.com	Pool1 InternalWebFQDN.contoso.com Pool2 InternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1 InternalWebFQDN.contoso.com Dialin.contoso.com alias to Pool2 InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Dialin-ext.geolb.contoso.com	Pool1 ExternalWebFQDN.contoso.com Pool2 ExternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1 ExternalWebFQDN.contoso.com Dialin.contoso.com alias to Pool2 ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Lyncdiscoverint-int.geolb.contoso.com	Pool1 InternalWebFQDN.contoso.com Pool2 InternalWebFQDN.contoso.com	Lyncdiscoverinternal.contoso.com alias to Pool1 InternalWebFQDN.contoso.com Lyncdiscoverinternal.contoso.com alias to Pool2 InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Lyncdiscover-ext.geolb.contoso.com	Pool1 ExternalWebFQDN.contoso.com Pool2 ExternalWebFQDN.contoso.com	Lyncdiscover.contoso.com alias to Pool1 ExternalWebFQDN.contoso.com Lyncdiscover.contoso.com alias to Pool2 ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure

GEODNS RECORD	POOL RECORDS	CNAME RECORDS	DNS SETTINGS (SELECT ONE OPTION)
Scheduler-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1InternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure
Scheduler-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools <b>OR</b> Use primary, connect to secondary if there's a failure

## DNS load balancing

DNS load balancing is usually implemented at the application level. The application (for example, a client running Skype for Business), tries to connect to a server in a pool by connecting to one of the IP addresses returned from the DNS A and AAAA (if IPv6 addressing is used) record query for the pool FQDN.

For example, if there are three Front End Servers in a pool named pool01.contoso.com, the following would happen:

- Clients running Skype for Business query DNS for pool01.contoso.com. The query returns three IP addresses and caches them as follows (in some order):

pool01.contoso.com	192.168.10.90
pool01.contoso.com	192.168.10.91
pool01.contoso.com	192.168.10.92

- The client tries to establish a TCP connection to one of the IP addresses. If that fails, it'll try the next IP address it's cached from that list.
- If the TCP connection succeeds, the client negotiates TLS to connect to the primary registrar on pool01.contoso.com.
- If the client tries all cached entries without a successful connection, the user receives a notification that no servers running Skype for Business Server are available at the moment.

### NOTE

DNS-based load balancing is different from DNS round robin (DNS RR), which typically refers to load balancing by relying on DNS to give a different order of IP addresses for the servers in your pool. Typically, DNS RR enables load distribution, but it won't allow you to enable failover. For example, if the connection to the one IP address returned by your DNS A (or AAAA in an IPv6 scenario) query fails, that connection will fail. That makes DNS RR less reliable than DNS-based load balancing. You can still use DNS RR in conjunction with DNS-based load balancing if you need to do that.

You use DNS load balancing to:

- Load balance server-to-server SIP to the Edge Servers.
- Load balance Unified Communication Application Services (UCAS) applications, such as Conferencing Auto Attendant, Response Group, and Call Park.
- Prevent new connections to UCAS applications (also known as draining).
- Load balance all client-to-server traffic between clients and Edge Servers.

You can't use DNS load balancing for:

- Client-to-server web traffic to your Front End Servers or a Director.

To go a little more in-depth on how a DNS SRV record's selected when multiple DNS records are returned by a query, the Access Edge service always picks the record with the lowest numeric priority and, if a tie-breaker is needed, the highest numeric weight. This is consistent with [Internet Engineering Task Force documentation](#).

So, for example, if your first DNS SRV record has a weight of 20 and a priority of 40, and your second DNS SRV record has a weight of 10 and a priority of 50, the first record's going to be chosen because it has the lower priority of 40. Priority always goes first, and that's the host that a client will target first. What if there are two targets with the same priority?

In that case, weight comes into consideration. Larger weights should be given a high probability, in this circumstance, of being selected. DNS administrators should use weight 0 when there isn't any server selection to do. In the presence of records containing weights greater than 0, records with weight 0 have a very small chance of being selected.

So, then, what happens if multiple DNS SRV records with equal priority and weight are returned? In this situation the Access Edge service will choose the SRV record that it got from the DNS server first.

# Edge Server scenarios in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Review these scenarios to help you plan your Edge Server topology in Skype for Business Server.

We have some scenarios diagrams to assist with visualizing and deciding on what Skype for Business Server Edge Server topology you want to implement. Once you've picked a good candidate, you can go read up on the environmental requirements you'll need to address. The following is applicable to any of the scenarios, so we're mentioning it first.

These figures, which are shown for example purposes only (and as such contains sample IPv4 and IPv6 data), don't represent the actual communication flow, but rather a high-level view of your possible traffic. Port details can also be seen in the Port diagrams for each scenario below.

The diagrams show .com for the external interface and .net for the internal, which is also sample material; of course your own entries may be quite different when you're putting together your own final Edge plan.

We don't include the Director (which is an optional component) in any of the diagrams, but you can read about that separately (it's mentioned in other Planning topics).

As noted above, there is sample IPv6 data in the diagrams. Most of the documentation in [Plan for Edge Server deployments in Skype for Business Server](#) will refer to IPv4, but you are certainly supported if you want to use IPv6. Note that you'll need IPv6 addresses in your assigned address space, and they'll need to work with internal and external addressing, as with IPv4 IPs. You can, thanks to Windows, employ the dual stack feature, which is a separate and distinct network stack for IPv4 and IPv6. This will, if you need, allow you to assign IPv4 and IPv6 addresses concurrently.

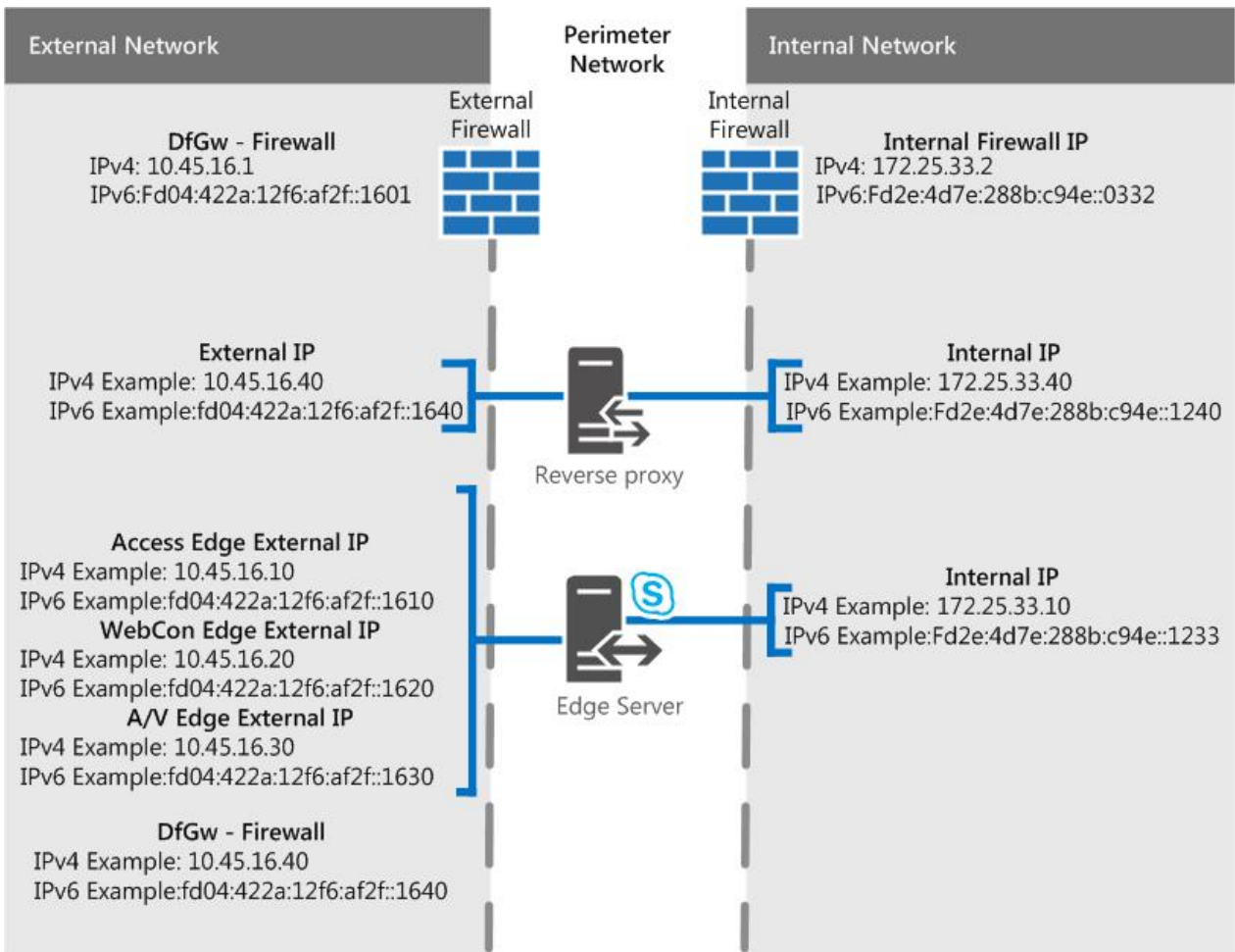
There are NAT devices that allow for NAT64 (IPv6 to IPv4) and NAT66 (IPv6 to IPv6)), and this is valid for use with Skype for Business Server.

## IMPORTANT

If you're using Call Admission Control (CAC) you do have to use IPv4 on the internal interface for it to work.

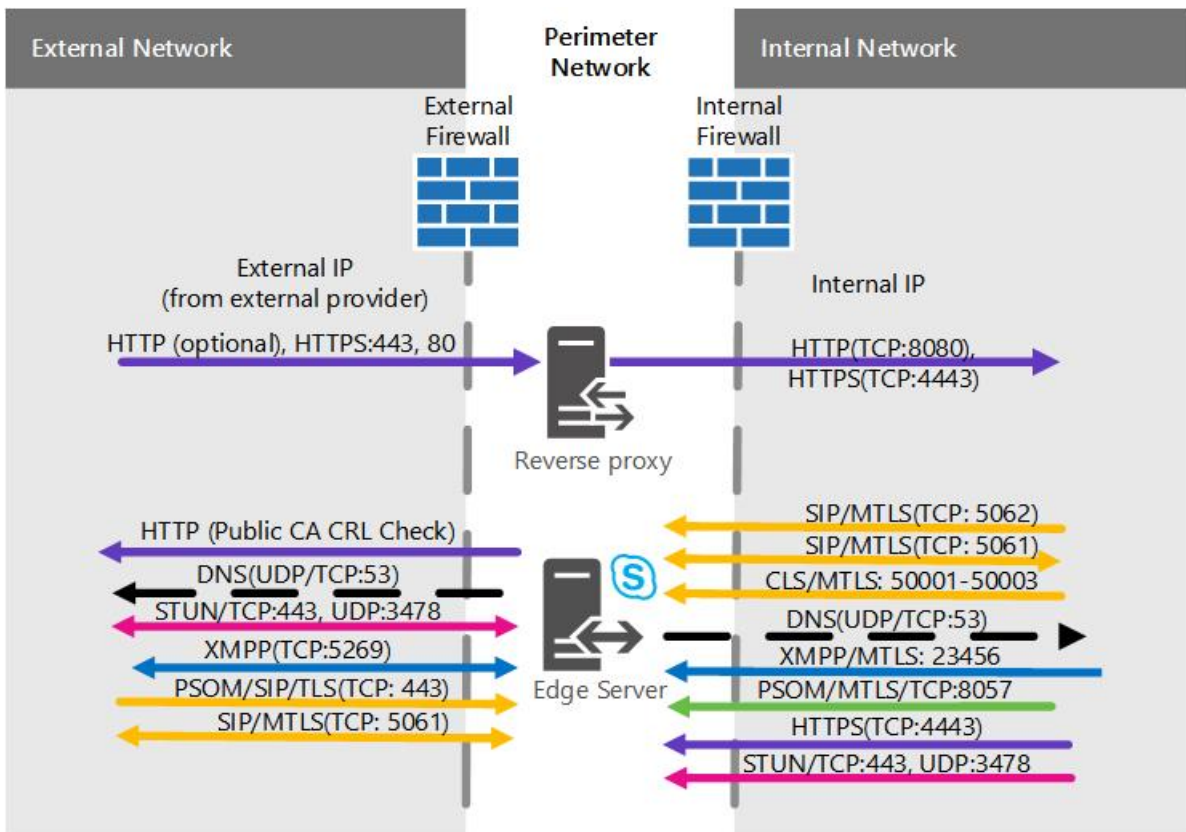
## Single consolidated Skype for Business Server Edge Server with private IP addresses and NAT

With this scenario, there is no option for high availability. This will mean you spend less on hardware and have a simpler deployment. If high availability is a must, check out the Scaled consolidated scenarios below.



**Port diagram**

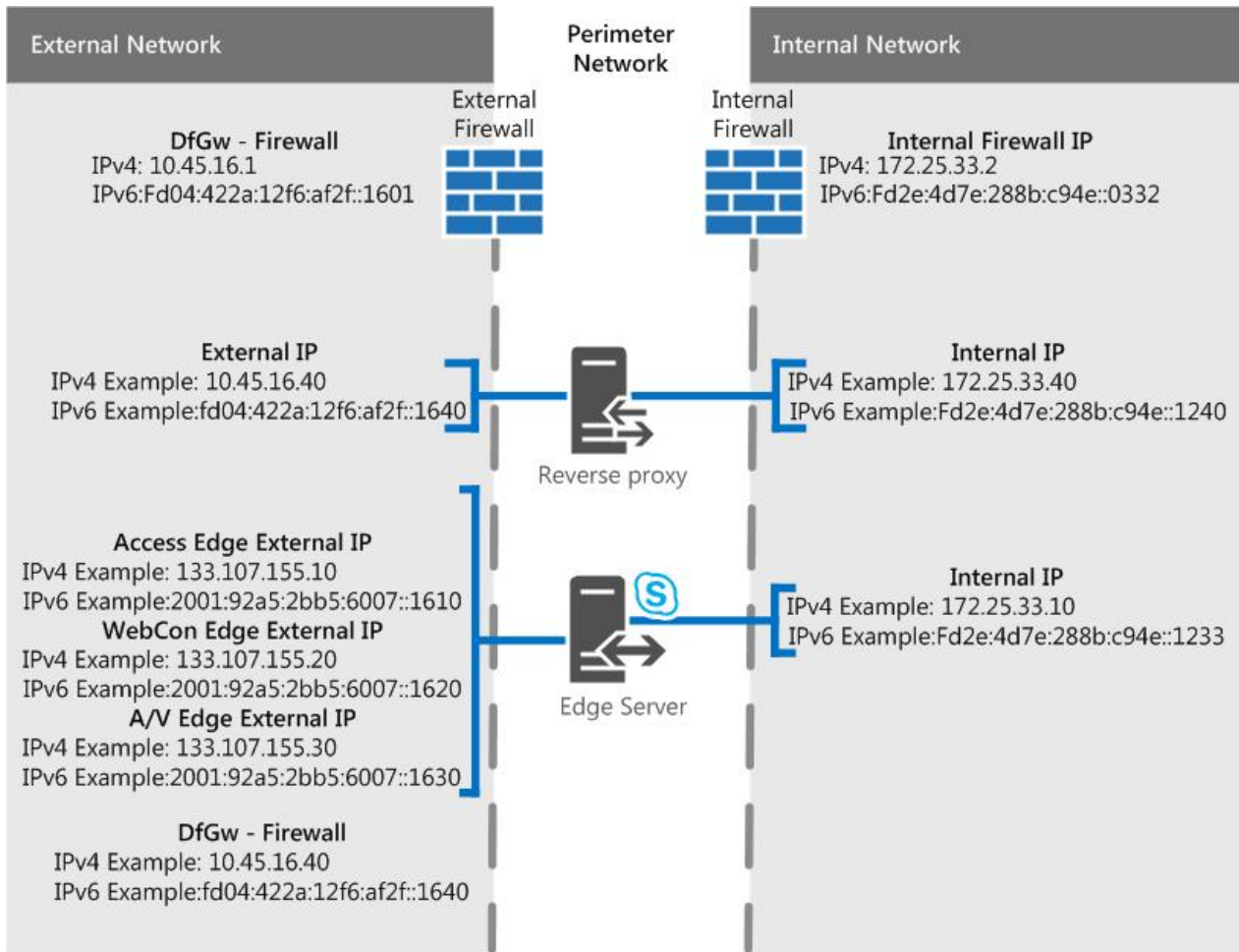
We also have a diagram for ports for single consolidated Edge Servers.



Single consolidated Skype for Business Server Edge Server with public

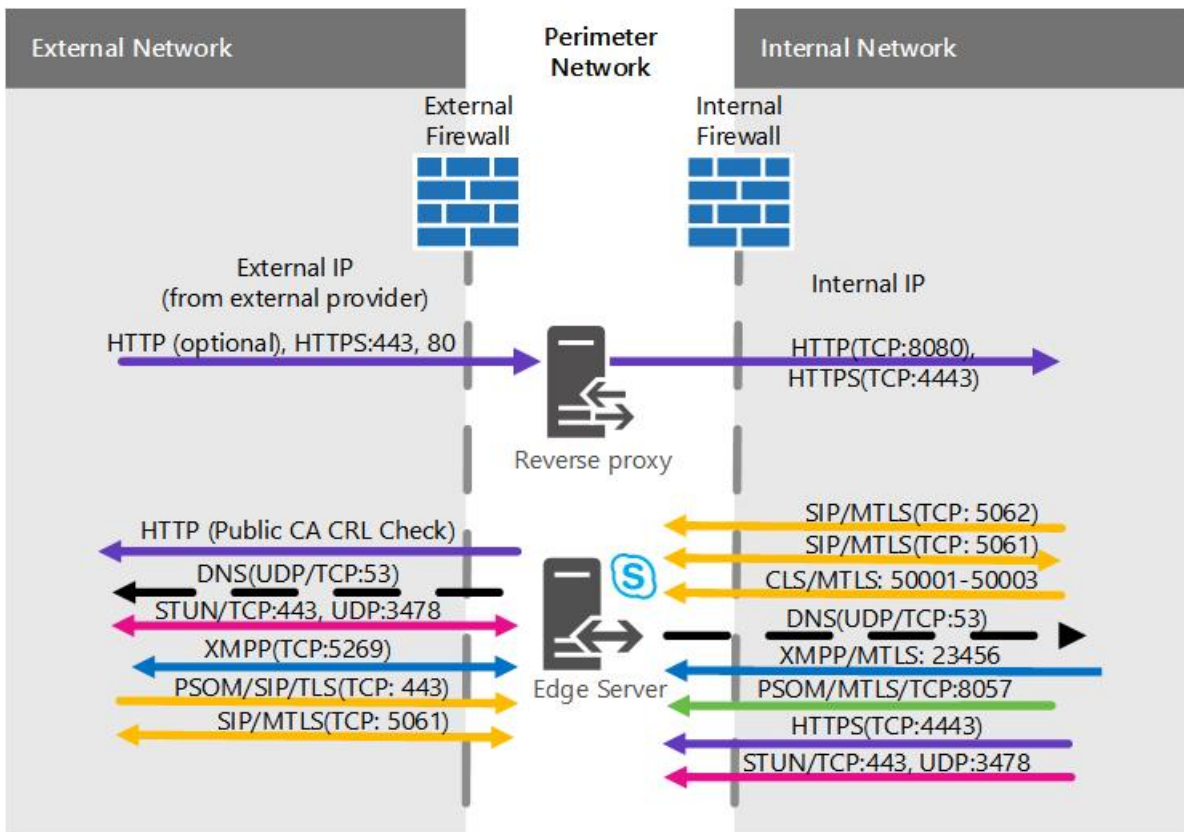
# IP addresses

With this scenario, there is no option for high availability. This will mean you spend less on hardware and have a simpler deployment. If high availability is a must, check out the Scaled consolidated scenarios below.



## Port diagram

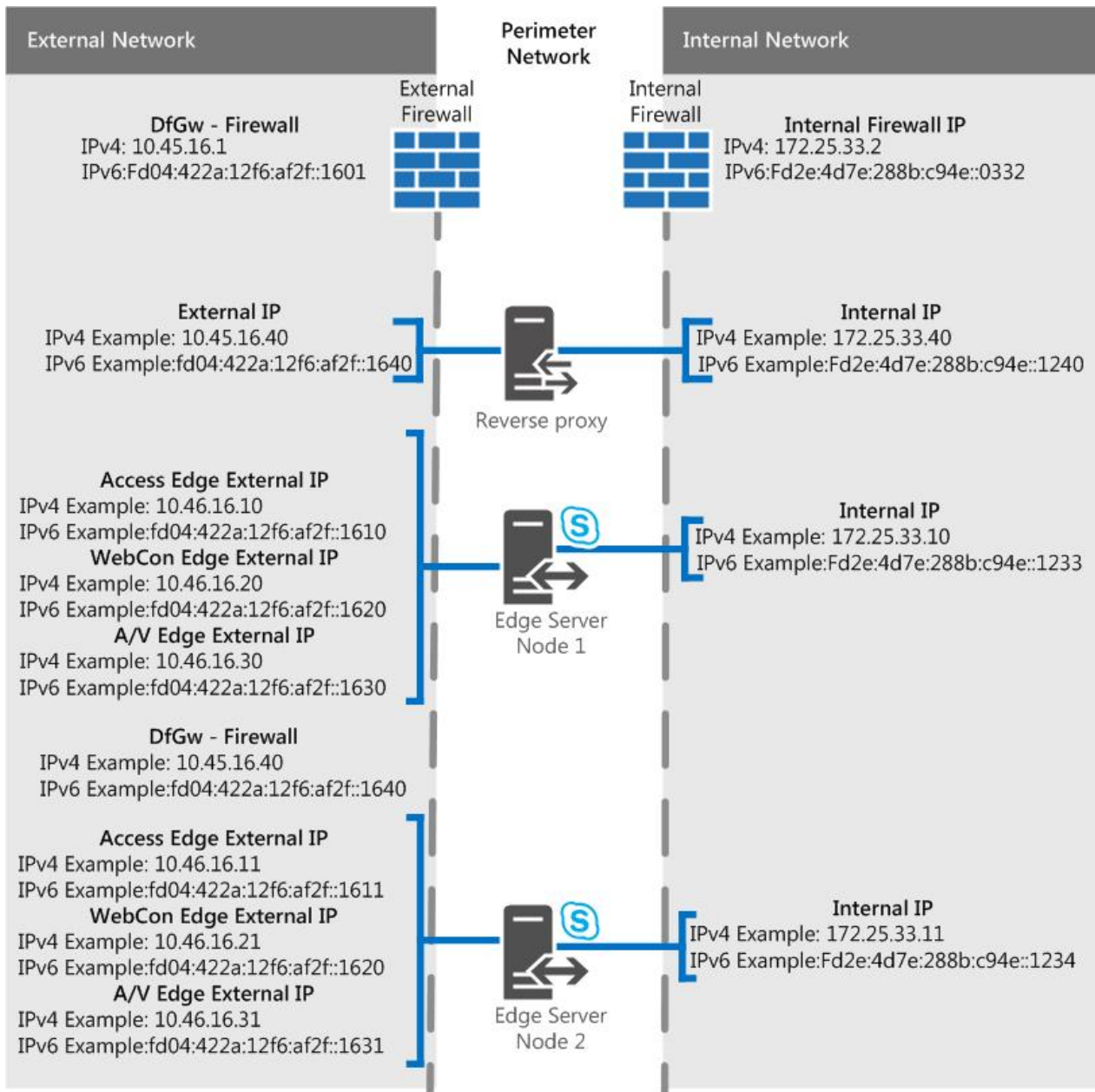
We also have a diagram for ports for single consolidated Edge Servers.



## Scaled consolidated Skype for Business Server Edge pool, with DNS load balancing, and private IP addresses and NAT

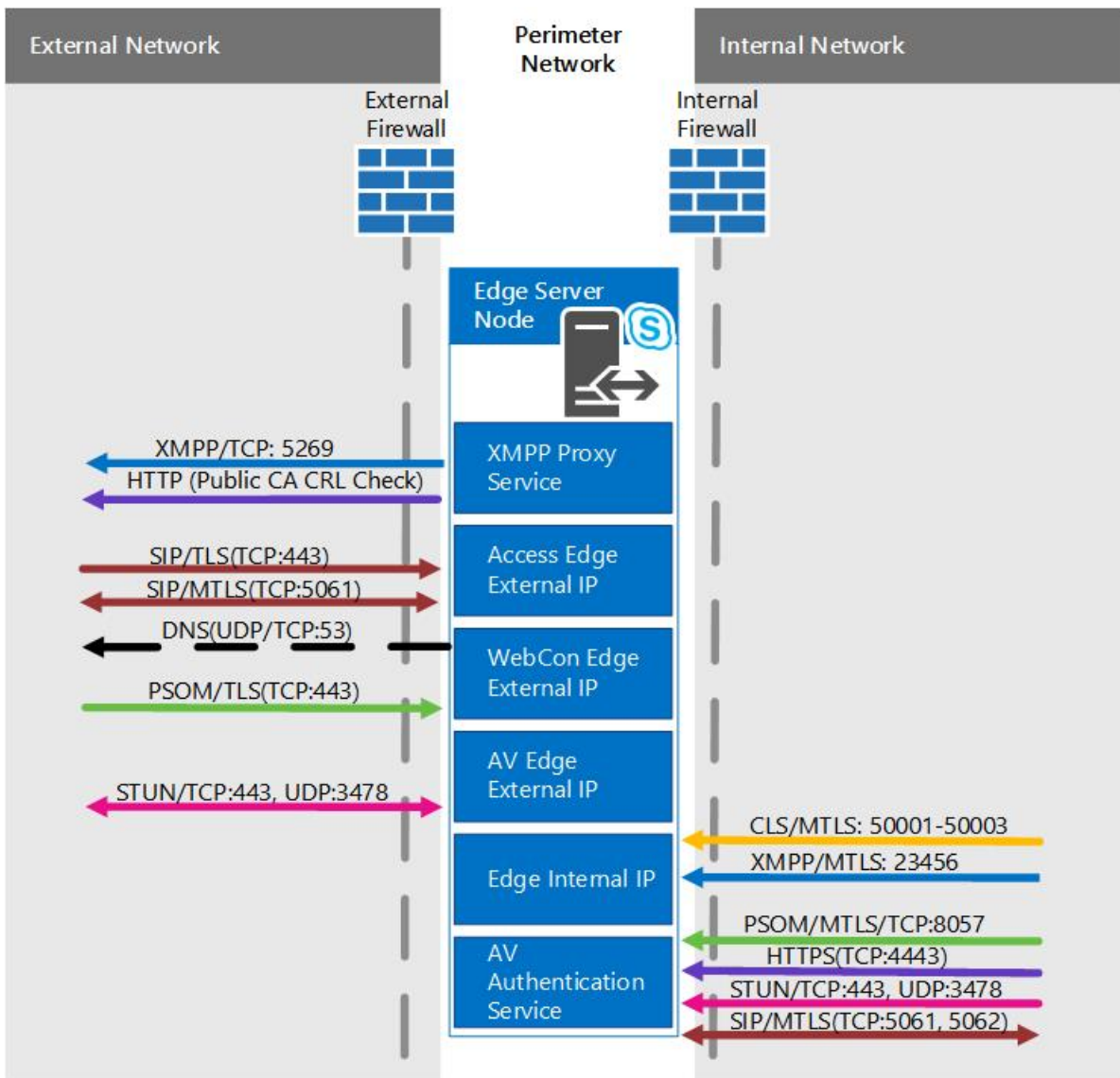
With this scenario, you are able to have high availability in your Edge deployment, which gives you the advantages of scalability and failover support.





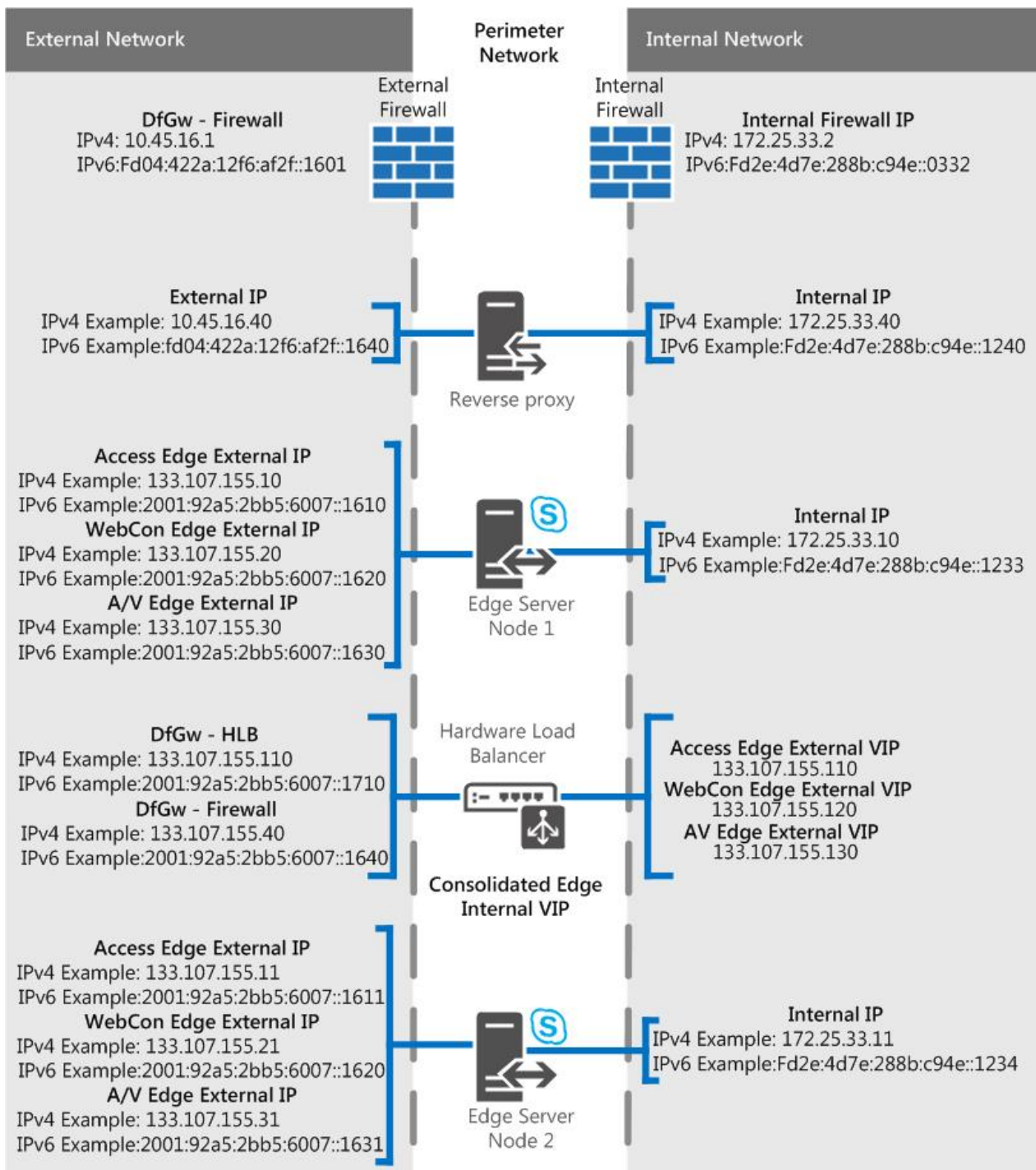
### Port diagram

We also have a diagram for scaled consolidated Edge pools with DNS load balancing.



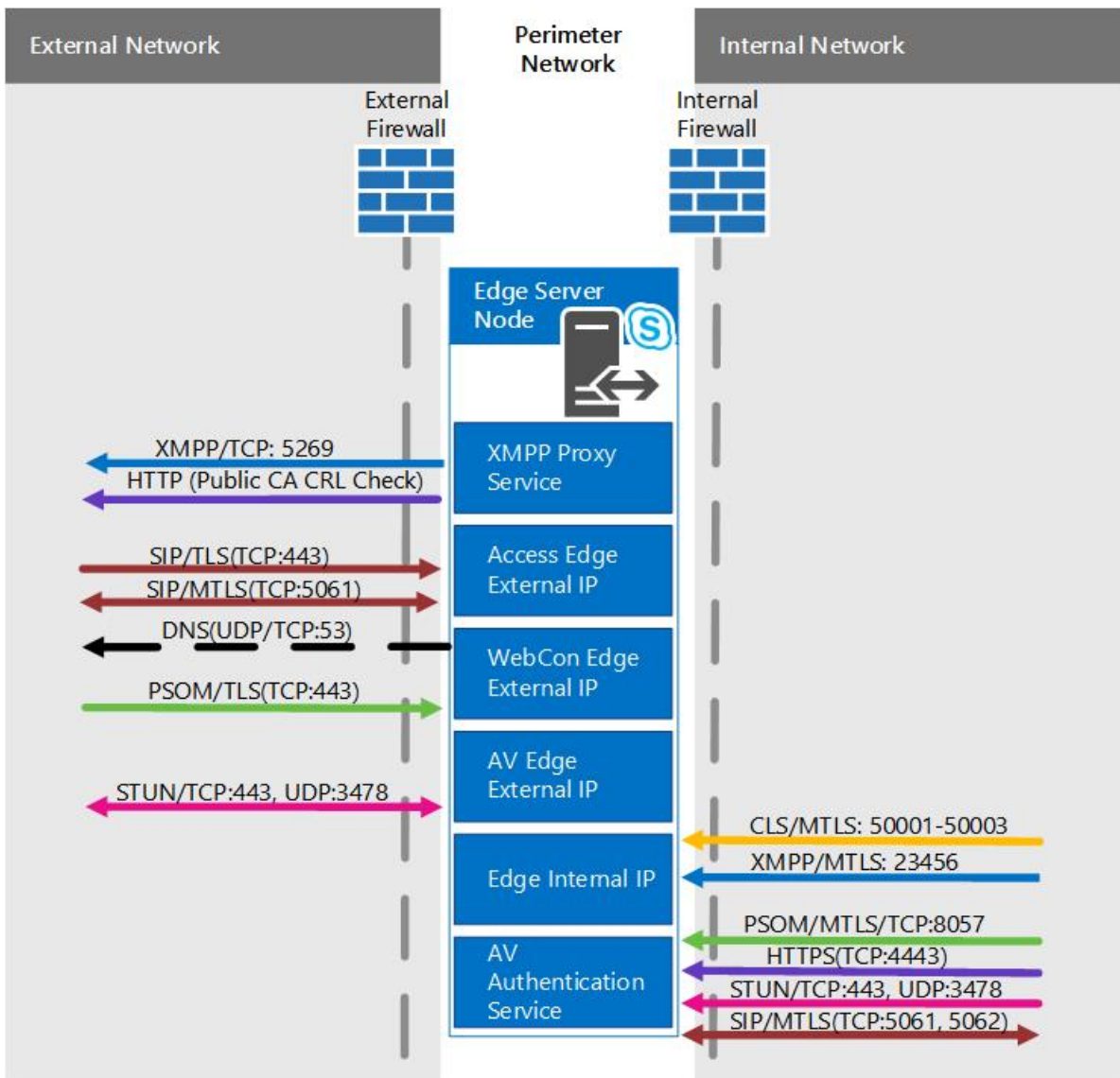
## Scaled consolidated Skype for Business Server Edge pool, with DNS load balancing and public IP addresses

With this scenario, you are able to have high availability in your Edge deployment, which gives you the advantages of scalability and failover support.



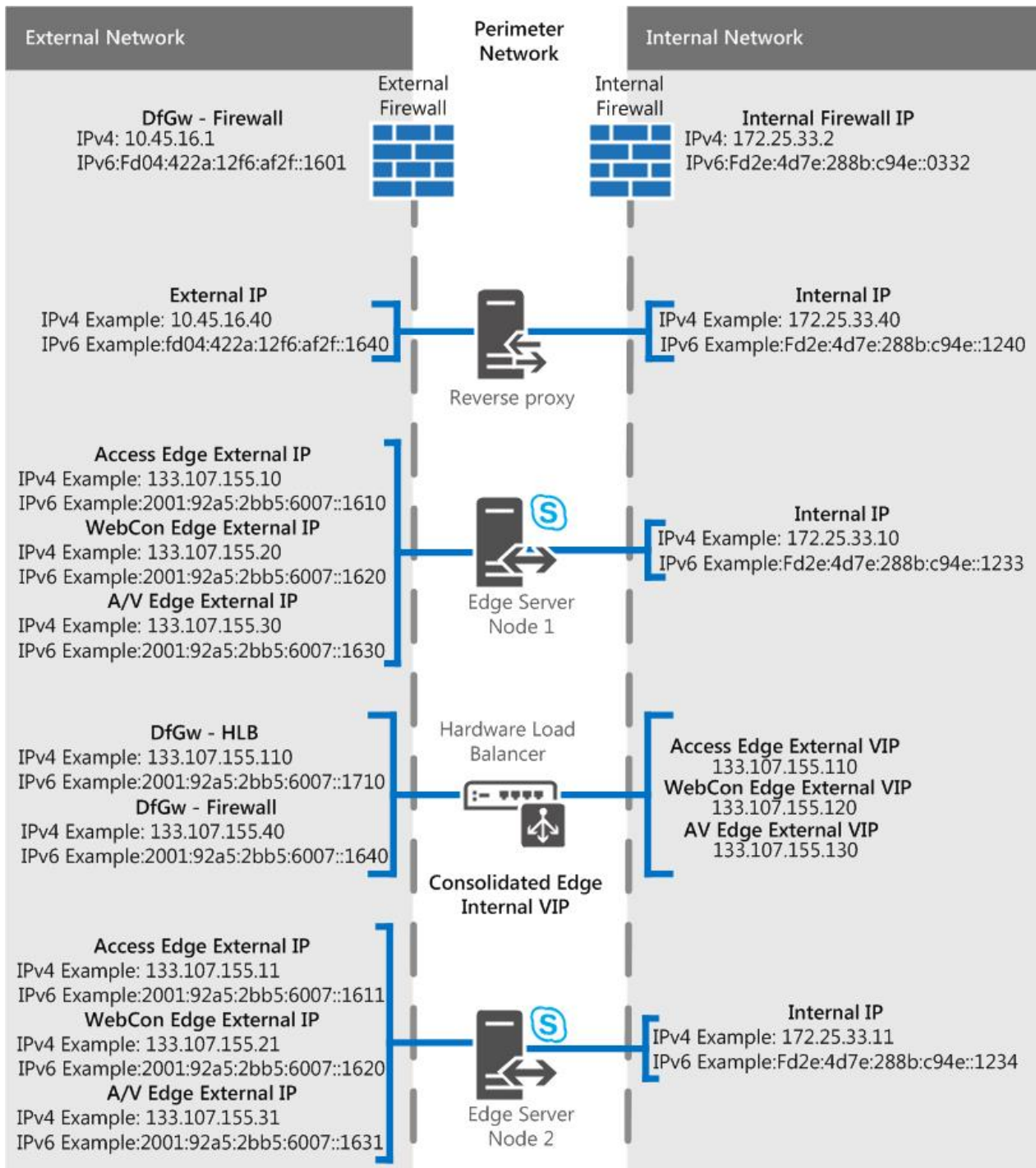
### Port diagram

We also have a diagram for scaled consolidated Edge pools with DNS load balancing.



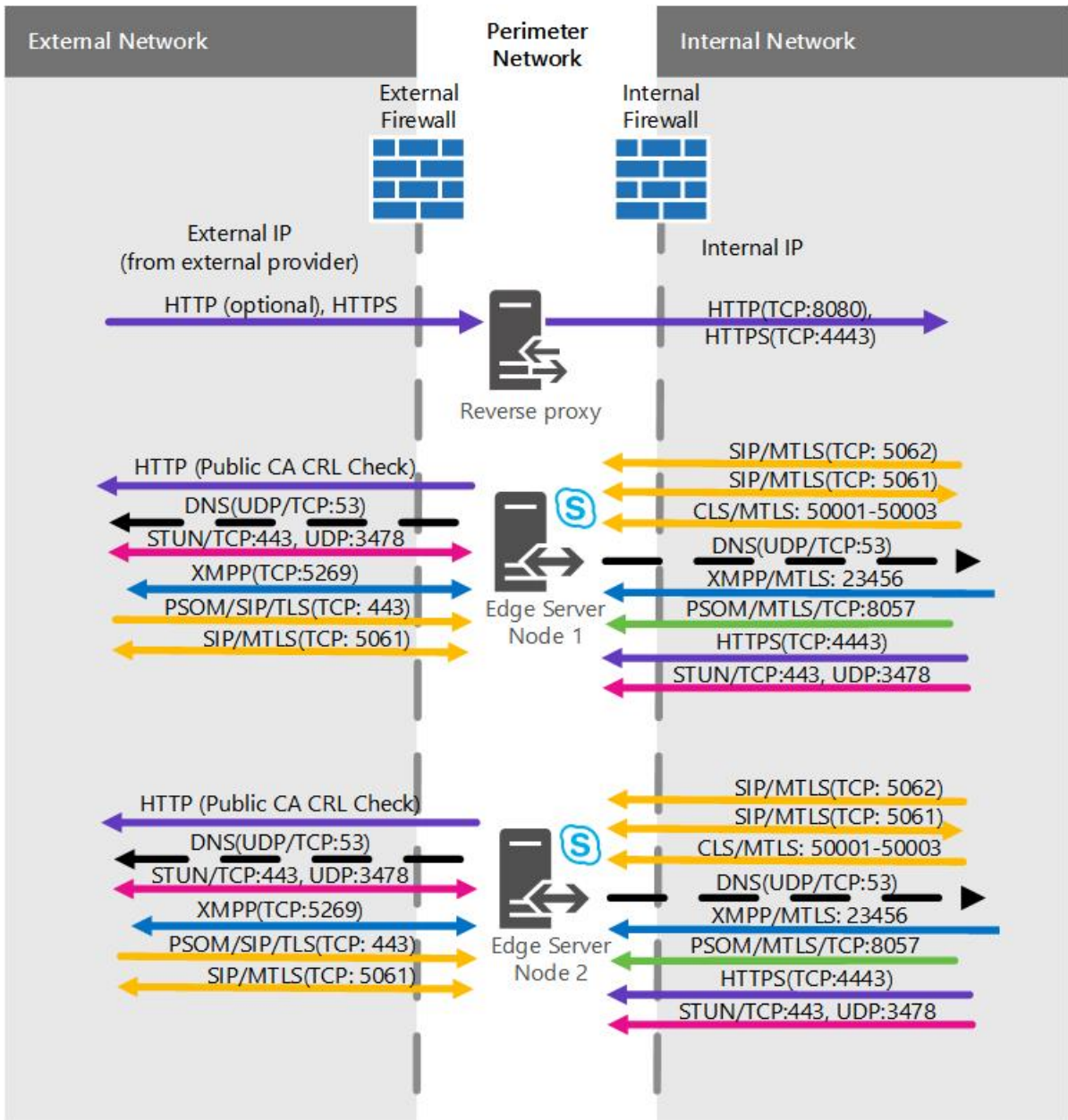
## Scaled consolidated Skype for Business Server Edge pool, with hardware load balancing

With this scenario, you are able to have high availability in your Edge deployment, which gives you the advantages of scalability and failover support.



### Port diagram

We also have a diagram for scaled consolidated Edge pools with hardware load balancing



# Plan for Mobility for Skype for Business Server

5/20/2019 • 16 minutes to read

Plan for your implementation of Mobility for Skype for Business Server.

With Skype for Business Server, you can deploy the Mobility feature to provide Skype for Business Server functionality on mobile devices. This article provides details about the Mobility feature, and helps you plan for your deployment.

The Mobility feature for Skype for Business Server is able to support mobile clients for Skype for Business, as well as Lync clients going back to 2010. Once it's deployed, your users can connect to your Skype for Business Server deployment using supported iOS, Android and Windows Phone mobile devices to take advantage of several different features, including Enterprise Voice features. We've included a partial list below, and you can also check [Desktop client feature comparison for Skype for Business](#) for more info:

- Send and receive messages
- View presence
- View contacts
- Click to join a conference
- Call via work
- Single number reach
- Voice mail
- Missed call notification
- Voice over IP (VoIP)
- Attendee video (H.264)
- Viewing meeting content (PowerPoint and desktop/application sharing)

All this is accomplished through the Unified Communications Web API, or UCWA. UCWA was first introduced in Lync Server 2013, and it's still in use for Skype for Business Server. There's an additional functionality for communicating with Lync 2010 clients, and that's Mobility Service (MCX). These are complimentary services, allowing for Lync Server 2010 and 2013 clients, as well as Skype for Business clients, to access Skype for Business Server deployments successfully.

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

It's important to note that while all these features are available once Mobility has been implemented, they may work a little differently on some devices. We've got a website that discusses what features work on what devices, at [Mobile client feature comparison for Skype for Business](#). We also have some great device and OS information at [Plan for clients and devices](#).

Mobility makes use of the Autodiscover feature, which allows clients to automatically locate Skype for Business

Server web services without users needing to enter in any URLs (they won't even need to know them). If you need to do some troubleshooting, manual entry of URLs is still supported.

Push notifications are also supported, for when the Skype for Business app isn't running in the background (or for mobile devices that don't support applications running in the background). A push notification is sent to a mobile device about an event that occurs when the device or app is inactive. A good example is missing an IM message when your phone's not active, which would result in a push notification being sent (this is presented as a toast or notification, like when the app is running in the background). With push notifications, users won't miss IM or voice calls.

For more information, we have the following sections:

- [Mobility components](#)
- [Supported topologies](#)
- [Technical requirements](#)
- [Defining your Mobility needs](#)

## Mobility components

There are four services that comprise Mobility for Skype for Business Server:

- **Unified Communications Web API (UCWA)**

Provides services for real-time communications with mobile and web clients for Skype for Business Server. When Skype for Business Server is deployed, a UCWA virtual directory's created in the internal and external web services. A virtual component in this virtual directory that accepts calls from UCWA-enabled clients. The client apps communicate over a representational state transfer (REST) interface for:

- presence
- contacts
- instant messaging (IM)
- VoIP
- video conferencing
- collaboration

UCWA uses a P-GET based channel to send events, such as an incoming call, incoming IM, or a message to the client app.

- **Mobility service (MCX)**

Supports Skype for Business Server functionality, such as IM, presence, and contacts, on mobile devices. The Mobility service is installed on every Front End Server in each pool that's intended to support Skype for Business Server functionality on mobile devices. When you install Skype for Business Server 2015 a new virtual directory (Mcx) is created under both the internal and external websites on your Front End Servers.

### NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.



- **Autodiscover service**

Identifies the location of the user and enables mobile devices and other Skype for Business clients to locate resources (such as the internal and external URLs for Skype for Business Server Web Services, the Mcx URL , or UCWA URL) regardless of network location. Automatic discovery uses hardcoded host names (lyncoverinternal for users inside the network, lyncover for users outside the network), and the SIP domain of the user. It supports client connections that use either HTTP or HTTPS.

The Autodiscover service is installed on every Front End Server and on every Director in each pool that's intended to support Skype for Business Server functionality on mobile devices. When you install the service, a new virtual directory (Autodiscover) is created under both the internal and external websites on your Front End Servers and Directors.

- **Push notification service**

A cloud-based service that's located in your Skype for Business Online data center. On phones that don't have Skype for Business client running in the background, when a new event happens, notification of a missed event (called a push notification) gets sent to the mobile device instead. The Mobility service sends a notification to the push notification service (MPNS), which then sends it to the mobile device. The user can then respond to the notification on their mobile device to activate the app. An Edge Server is required for this functionality.

## Supported topologies

We have the following supported Skype for Business Server applications for your topology planning:

- Mobility Standard Edition
- Mobility Enterprise Edition

You should be able to use this functionality with Skype for Business Server Edge Servers or Lync Server 2013 Edge Servers.

The Mobility service is supported on Front End Servers when collocated with the Mediation Server role, with two network interfaces, but you need to take appropriate steps to configure those interfaces. You'll need to assign IP addresses to the specific interface that will communicate as the Mediation Server, and the network IP interface that will communicate as the Front End Server. You can do this in Topology Builder by selecting the correct IP address for each service, instead of using the default **Use all configured IP addresses** selection.

## Technical requirements

It's important to plan for the various mobile application scenarios your mobile users may encounter. For example, someone might start using a mobile app outside of work by connecting through a 3G network, then switch to the corporate Wi-Fi network when they reach work. They may switch to 4G when leaving their building. Planning now will allow you to support these network transitions and guarantee a consistent user experience.

### **DNS configuration**

The Mobility services Mcx and UCWA use DNS in the same way. With Automatic Discovery, mobile devices use DNS to locate resources. During DNS lookup, a connection's attempted to the FQDN that's associated with the internal DNS record (lyncoverinternal.[internal domain name]). If the internal DNS record can't be used to make that connection, a second connection is attempted, this time to the external DNS record (lyncover.[sipdomain]). So why have two? A mobile device that's internal to your network will be able to use the internal Autodiscover URL. External mobile devices will use the external Autodiscover URL. In either case, the Autodiscover service will return all Web service URLs for the user's home pool, which includes the Mobility service (Mcx and UCWA).

It's expected that the external Autodiscover requests will go through the reverse proxy you've configured for Skype for Business Server. However, both the internal Mobility service URL and the external Mobility service URL are associated with the external Web Services FQDN. Therefore, regardless of whether a mobile device is internal or external to your network, the device always connects to the Skype for Business Server Mobility service externally, through your reverse proxy.

#### NOTE

As we just noted, all Mobility service traffic (internal and external) will go through your reverse proxy. But sometimes an issue comes up when the internal traffic leaves through an interface, only to then try and come back in on the same interface. This can violate your spoofing (formally it's called TCP packet spoofing) security rules. You'll need to allow **Hair Pinning** to have Mobility function.

#### NOTE

If you're ready to do this, you can also choose to use a reverse proxy that's separate from your firewall (for security purposes, spoofing prevention should always be enforced at your firewall). This way, the hairpin can happen at the external interface of your reverse proxy, rather than your firewall's external interface. This allows you to detect the spoofing properly at your firewall while you relax the rule at your reverse proxy, and you get your Mobility functionality.

#### NOTE

If you go this route, be sure to use the DNS host or CNAME records to define the reverse proxy for the hairpin behavior (not the firewall), if possible.

There are some things you'll need to configure to support users inside and outside your corporate network.

These are the rules for internal and external web FQDNs:

- New CNAME or A (host, if IPv6, AAAA) DNS records, for automatic discovery.
- New firewall rule, if you want to support push notifications through your Wi-Fi network.
- Subject alternative names on internal server certificates and reverse proxy certificates, for automatic discovery.
- Front End Server hardware load balanced configuration changes source affinity.

These are the topology requirements needed to support the Mobility Service and Autodiscover Service:

- The Front End pool internal web FQDN must be distinct from the Front End pool external web FQDN.
- The internal web FQDN must only resolve to, and be accessible from, inside the corporate network.
- The external web FQDN must only resolve to, and be accessible from, the internet.
- For a user inside the corporate network, the Mobility service URL must be addressed to the external web FQDN. This requirement is for the Mobility service, and applies only to this URL.
- For a user outside the corporate network, the request must go to the external web FQDN of the Front End pool or Director.

If you support automatic discovery, you'll need to make the following DNS records for each SIP domain:

- An internal DNS record to support mobile users who connect from inside your organization's network.
- An external, or public, DNS record to support mobile users who connect from the internet.

The internal automatic discovery URL shouldn't be addressable from outside your internal network. The external automatic discovery URL shouldn't be addressable from within your network. But if this isn't possible for the external URL, your mobile client functionality probably won't be affected, because the internal URL will always be tried first.

### Port and Firewall requirements

We've covered most of this in our other documentation, but specifically for Mobility, you're going to want to have the following ports open on your enterprise Wi-Fi network if you have any users homed on a Survivable Branch Appliance (SBA):

- UcwaSipExternalListeningPort requires 5088.
- UcwaSipPrimaryListeningPort requires 5089.

### Certificate requirements

If you're using automatic discovery for your Skype for Business mobile clients, you'll need to modify the SAN (subject alternative name) lists on your certificates to support secure connections from your mobile clients. If you already have certificates in-place, you'll need to request and assign new certificates with the SAN entries described here. This will need to be done for each Front End Server and Director (if in your environment) that runs the Autodiscover service. We'd also recommend modifying the SAN lists on your reverse proxy certificates, adding SAN entries for every SIP domain in your organization.

This should be a straightforward process if you're requesting the new certs off an internal CA (certificate authority), but public certificates are more complex, and potentially a lot more expensive to re-request, not to mention it may be costly to add a lot of SIP domains to a new public cert. In that situation, there is an approach that's supported, but **not recommended**. You can configure your reverse proxy to make the initial Autodiscover service request over port 80, which will use HTTP, rather than port 443, which is HTTPS (and 443 is the default configuration). That incoming request will be redirected to port 8080 on your Front End pool or Director. By doing this, you won't need to make any certificate changes, because this traffic isn't using HTTPS for requests. But again, we don't recommend this, although it will work for you.

### Windows and IIS requirements

You should have a supported Windows Server version for your Skype for Business Server environment. As a result, you should also have IIS 8 or IIS 8.5 for your mobility needs. There will need to be some changes to the default ASP.NET settings, but the Mobility service installer will do that automatically.

### HLB requirements

If you're using a topology for Skype for Business Server that includes an HLB for your Front End pool (which would be any topology that includes more than one Front End Server), the external Web Services virtual IPs (VIPs) for Web Services traffic need to be configured for source. Source affinity helps to ensure that multiple connections from a single client are sent to the same server to maintain session state.

If you plan to support Skype for Business mobile clients only over your internal Wi-Fi network, you should configure your internal Web Services VIPs for source as described for external Web Services VIPs. In this situation, you should use source\_addr (or TCP) affinity for the internal Web Services VIPs on the HLB.

For details on all this, please review the [Load balancing requirements for Skype for Business](#) documentation.

### Reverse Proxy requirements

In order to support automatic discovery for Skype for Business mobile clients, you'll need to update the current publishing rule as follows:

- If you decide to update the SAN lists on your reverse proxy certificates, and you're using HTTPS for the initial Autodiscover service request, you need to update the web publishing rule for lyncdiscover.  
<sipdomain>. This is typically combined with the publishing rul for the external Web Services URL on the Front End pool.

- If you've decided to use HTTP for the initial Autodiscover service request to avoid having to update the SAN list for your reverse proxy certificates (which we don't recommend), you'll need to create a new web publishing rule for port HTTP/TCP 80, if there isn't one already. If that rule exists, update it to include a `lyncdiscover.<sipdomain>` entry.

## Defining your Mobility needs

Now that we've reviewed the topologies, components and technical requirements, let's look at what your organization may need in terms of a Mobility implementation.

### Do you want to use automatic discovery for Skype for Business mobile clients?

We do strongly recommend that you do use automatic discovery. It will require the creation of new internal and external DNS records, as documented in the Technical Requirements section above. With automatic discovery, the Skype for Business clients can automatically locate Skype for Business Server Web Services from any location, without needing a URL to be entered in manually.

You can use manual settings if you need to. These URLs will need to be entered by users into their mobile devices:

- **`https://<ExtPoolFQDN>/Autodiscover/autodiscover.service.svc/Root`** for external access.
- **`https://<IntPoolFQDN>/Autodiscover/autodiscover.service.svc/Root`** for internal access.

Again, we do recommend using automatic discovery. You may find manual settings useful for troubleshooting purposes.

### Are you going to support push notifications?

Push notifications are used for mobile applications that support this functionality to notify a user of events while the app's not active. Your Edge Server will need to have a federation relationship with your cloud-based Skype for Business Server Push Notification Service, which is found on the Skype for Business Online datacenter. You'll need to run a cmdlet to enable push notifications.

#### NOTE

If you have anyone still using Lync Server 2010 clients, they will need TCP port 5223 open outbound on your enterprise WiFi network.

### Do you want all your users accessing all Mobility features, or do you want to specify the users who can access these features instead?

We have a table to help with some of the features that are available to all users, and whether they're set that way or not by default. For a complete list, please review [New-CsMobilityPolicy](#).

#### NOTE

The scopes for all these features are Global/Site/User.

FEATURE	PARAMETER NAME	DESCRIPTION	DEFAULT SETTING
Enable Mobility	EnableMobility	Controls users in a given scope who have Skype for Business mobile client installed. If the policy is set to False, your users won't be able to sign in with their client.	True

FEATURE	PARAMETER NAME	DESCRIPTION	DEFAULT SETTING
Outside Voice	EnableOutsideVoice	Enables a user's ability to use Call Via Work, which lets users send and receive calls by using their work number instead of their mobile number. If it's set to False, your users won't be able to make or receive calls on their mobile phone when using their work phone number.	True
Enable IP Audio and Video	EnableIPAudioVideo	Set to the default, it allows a user to use VoIP to make or receive phone or video calls on their mobile device. When set to False, your users won't be able to use their mobile device to do either of those things.	True
Require WiFi for IP Audio	RequireWiFiForIPAudio	Defines whether a client will need to make and receive calls over VoIP on WiFi instead of a cellular data network. If it's set to True, your users will only be able to make and receive VoIP calls when they're connected via WiFi.	False
Require WiFi for IP Video	RequireWiFiForIPVideo	Defines whether a client will need to make and receive video calls on WiFi instead of a cellular data network. If it's set to True, your users will only be able to make and receive VoIP calls when they're connected via WiFi.	False

### Should users who aren't enabled for Enterprise Voice be able to use Click to Join to join conferences?

For users to have access to Mobility features and Call via Work, they need to be enabled for Enterprise Voice. But even if they aren't enabled, they can still join conferences by clicking on a link on their mobile device, but only if they have an appropriate Voice policy assigned to them. You can either:

- assign a specific Voice policy to these users, or,
- make sure that a global policy or site-level policy exists and applies to them.

Either way, the Voice policy you assign needs to have public switched telephone network (PSTN) usage records and routes that will define where your users will be able to dial out to join conferences.

#### NOTE

Mobile users who want to use Click to Join require a Voice policy, along with the related PSTN usage records and voice routes, because when they click on that link on their mobile devices, an outbound call from Skype for Business Server will be the result.



# Plan for security in Skype For Business Server

5/20/2019 • 2 minutes to read

Skype for Business Server security content.

This content relates to Skype for Business Server security. Security is a very broad topic. Security reaches across every feature of Skype for Business Server as well as databases, services, and hardware that make up the ecosystem. This content is a supplement for specific security topics regarding Skype for Business Server.

## In This Section

- [Antivirus scanning exclusions for Skype for Business Server](#)
- [Key security features in Skype for Business Server](#)
- [Common security threats in modern day computing](#)
- [Security framework for Skype for Business Server](#)
- [Addressing threats to your core infrastructure for Skype for Business Server](#)

# Antivirus scanning exclusions for Skype for Business Server

11/8/2019 • 2 minutes to read

Overview of antivirus scanner interoperation with Skype for Business Server.

To ensure that the antivirus scanner does not interfere with the operation of Skype for Business Server, you must exclude specific processes and directories for each Skype for Business Server server or server role on which you run an antivirus scanner. The following processes and directories should be excluded:

## NOTE

Folder and file locations listed below are the default locations for Skype for Business Server. For any locations for which you did not use the default, exclude the locations you specified for your organization instead of the default locations specified in this topic.

## IMPORTANT

Please note that some antivirus programs may need absolute, not relative paths, for their exclusion list.

- Skype for Business Server processes:
  - ABServer.exe
  - ASMCUSvc.exe
  - AVMCUSvc.exe
  - ChannelService.exe
  - ClsAgent.exe
  - ComplianceService.exe
  - DataMCUSvc.exe
  - DataProxy.exe
  - FileTransferAgent.exe
  - HealthAgent.exe
  - IMMCUSvc.exe
  - LyncBackupService.exe
  - LysSvc.exe
  - MasterReplicatorAgent.exe
  - MediaRelaySvc.exe
  - MediationServerSvc.exe
  - MRASSvc.exe



- OcsAppServerHost.exe
- ReplicaReplicatorAgent.exe
- ReplicationApp.exe
- RtcHost.exe
- RTCSrv.exe
- XmppProxy.exe
- XmppTGW.exe
- Windows Fabric Host Service processes:
  - Fabric.exe
  - FabricDCA.exe
  - FabricHost.exe
- IIS processes:
  - %systemroot%\system32\inetsrv\w3wp.exe
  - %systemroot%\SysWOW64\inetsrv\w3wp.exe
- SQL Server Back-End processes:

**NOTE**

Note that these paths are specific to SQL Server version.

- %ProgramFiles%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSRS11.MSSQLSERVER\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSAS11.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- SQL Server Front-End processes:
  - %ProgramFiles%\Microsoft SQL Server\MSSQL12.LYNCLOCAL\MSSQL\Binn\SQLServr.exe
  - %ProgramFiles%\Microsoft SQL Server\MSSQL12.RTCLocal\MSSQL\Binn\SQLServr.exe
  - Standard Edition Installation RTC Instance
  - %ProgramFiles%\Microsoft SQL Server\MSSQL12.RTC\MSSQL\Binn\SQLServr.exe
- Directories and files:
  - %systemroot%\System32\LogFiles
  - %systemroot%\SysWow64\LogFiles
  - %systemroot%\Microsoft.NET\assembly\GAC\_MSIL

**NOTE**

Note that these paths are specific to Skype for Business Server version.

- %programfiles%\Skype for Business Server 2015
- %programfiles%\Common Files\Skype for Business Server 2015\Watcher Node
- %programfiles%\Common Files\Skype for Business Server 2015
- %programfiles%\Common Files\Skype for Business Online
- %SystemDrive%\RtcReplicaRoot
- File share store (specified in Topology Builder). File stores are specified in Topology Builder.
- SQL Server data and log files, including those for the back-end database, user store, archiving store, monitoring store, and application store. Database and log files can be specified in Topology Builder. For details about the data and log files for each database, including default names, see [SQL Server Data and Log File Placement](#) in the Deployment documentation.
- SQL Server data and log files, including those for the Front-end database, Skype for Business store, and RtcDatabase store. They are normally under %localdrive%\CSData.

# Key security features in Skype for Business Server

5/20/2019 • 5 minutes to read

Skype for Business Server includes several security features, including server-to-server authentication, role-based access control, and centralized storage of configuration data.

This article provides a high level overview of Skype for Business Server security.

## Key Security Features in Skype for Business Server

Security is a very broad topic. Security reaches across every feature of Skype for Business Server as well as databases, services, and hardware that make up a Skype for Business Server ecosystem. This article outlines some of the features in Skype for Business Server in particular that are designed for security.

### Planning and Design Tools

Skype for Business Server provides two tools to facilitate planning and design and to reduce the chance of mis-configuring Skype for Business Server components.

- **Topology Planning Tool** automates much of the topology design process. You can export the results from the Planning Tool to Topology Builder, which is the tool that is required to install each server running Skype for Business Server.
- **Topology Builder** stores all configuration information in the Central Management store.

For details about these tools, see [Skype for Business Server Management Tools](#).

### Central Management Store

In Skype for Business Server, configuration data about servers and services is part of the Central Management store. The Central Management store provides a robust, schematized storage of the data needed to define, set up, maintain, administer, describe, and operate a Skype for Business Server deployment. It also validates the data to ensure configuration consistency. All changes to this configuration data happen at the Central Management store, eliminating "out-of-sync" issues.

Read-only copies of the data are replicated to all servers in the topology, including Edge Servers and Survivable Branch Appliances. Replication is managed by a service that is, by default, run under the context of the Network service, reducing the rights and permissions to that of a simple user on the computer.

### Server-to-Server Authentication

In Skype for Business Server, authentication can be configured between servers by using the Open Authorization (OAuth) protocol. For example, you can configure Skype for Business Server to authenticate with a server that is running Microsoft Exchange Server 2016. Using the OAuth protocol, the Skype for Business Server and the Microsoft Exchange Server can trust each other. This provides the ability to integrate the products in a seamless manner. For details, see [Manage server-to-server authentication \(OAuth\) and partner applications in Skype for Business Server](#).

### Windows PowerShell-based management and Web-based Management Interface

Skype for Business Server provides a powerful management interface, built on the Windows PowerShell command-line interface. It includes cmdlets for managing security, and Windows PowerShell security features are enabled by default so that users cannot easily or unknowingly run scripts. This means that the software defaults are set to automatically help maximize security and reduce the avenues of attack. For details about Windows PowerShell management support in Skype for Business Server, see [Skype for Business Server Management Shell](#).

## Role-Based Access Control (RBAC)

Skype for Business Server provides role-based access control (RBAC) to enable you to delegate administrative tasks while maintaining high standards for security. You can use RBAC to follow the principle of "least privilege," in which users are given only the administrative rights that their jobs require. Skype for Business Server provides the ability to create a new role and also the ability to modify an existing role.

## Network Address Translation (NAT)

Skype for Business Server does not support the use of network address translation (NAT) on the internal interface of the Edge Server, but it does support placing the external interface of the Access Edge service, Web Conferencing Edge service, and A/V Edge service behind a router or firewall that performs network address translation (NAT) for both single and scaled consolidated Edge Server topologies. Multiple Edge Servers behind a hardware load balancer cannot use NAT. If multiple Edge Servers use NAT on their external interfaces, Domain Name System (DNS) load balancing is required. In turn, using DNS load balancing allows you to reduce the number of public IP addresses per Edge Server in an Edge Server pool. For details, see [Edge Server scenarios in Skype for Business Server](#).

### NOTE

If you federate with enterprises that have a Microsoft Office Communications Server 2007 deployment and you need to use audio/video between your enterprise and the federated enterprise, the port requirements will be those for the older version of the Edge Servers that are deployed. For example, the port ranges required for those older versions must be opened for both enterprises until the federated partner upgrades its Edge Servers to Skype for Business Server. At that time, the port requirements can be reviewed and reduced according to the new configuration.

## Simplified Certificates for Edge Servers

The Deployment Wizard can automatically populate subject names (SNs) and subject alternative names (SANs), reducing the possibility of including unnecessary and potentially unsecure entries.

## Trustworthy Computing Security Development Lifecycle (SDL)

Skype for Business Server is designed and developed in compliance with the [Microsoft Trustworthy Computing Security Development Lifecycle](#) (SDL).

- **Trustworthy by Design** The first step in creating a more secure unified communications system was to design threat models and test each feature as it was designed. In addition, Microsoft performs testing outside of the designed behavior in order to find security vulnerabilities resulting from unexpected product behavior. Multiple security-related improvements were built into the coding process and practices. Build-time tools detect buffer overruns and other potential security threats before the code is checked in to the final product. Of course, it is impossible to design against all unknown security threats. No system can guarantee complete security. However, because product development embraced secure design principles from the start, Skype for Business Server incorporates industry standard security technologies as a fundamental part of its architecture.
- **Trustworthy by Default** By default, network communications in Skype for Business Server are encrypted. Because all servers use certificates and Kerberos authentication, TLS, Secure Real-Time Transport Protocol (SRTP), and other industry-standard encryption techniques, including 128-bit Advanced Encryption Standard (AES) encryption, virtually all Skype for Business Server data is protected on the network. In addition, role-based access control makes it possible to deploy servers running Skype for Business Server so that each server role runs only the services, and has only the permissions related to those services, that are appropriate for the server role.
- **Trustworthy by Deployment** All Skype for Business Server documentation includes best practices and

recommendations to help you determine and configure the optimal security levels for your deployment and assess the security risks of activating non-default options.

# Common security threats in modern day computing

5/20/2019 • 7 minutes to read

Because Skype for Business Server is an enterprise-class communications system, you should be aware of common security attacks that could affect its infrastructure and communications.

## Compromised-Key Attack

A key is a secret code or number that is used to encrypt, decrypt, or validate secret information. There are two sensitive keys in use in public key infrastructure (PKI) that must be considered:

- The private key that each certificate holder has
- The session key that is used after a successful identification and session key exchange by the communicating partners

A compromised-key attack occurs when the attacker determines the private key or the session key. When the attacker is successful in determining the key, the attacker can use the key to decrypt encrypted data without the knowledge of the sender.

Skype for Business Server uses the PKI features in the Windows Server operating system to protect the key data used for encryption for the Transport Layer Security (TLS) connections. The keys used for media encryption are exchanged over TLS connections.

## Network Denial-of-Service Attack

The denial-of-service attack occurs when the attacker prevents normal network use and function by valid users. This is done when the attacker floods the service with legitimate requests that overwhelm the use of the service by legitimate users. By using a denial-of-service attack, the attacker can do the following:

- Send invalid data to applications and services running in the attacked network to disrupt their normal function.
- Send a large amount of traffic, overloading the system until it stops responding or responds slowly to legitimate requests.
- Hide the evidence of the attacks.
- Prevent users from accessing network resources.

## Eavesdropping (Sniffing, Snooping)

Eavesdropping can occur when an attacker gains access to the data path in a network and has the ability to monitor and read the traffic. This is also called sniffing or snooping. If the traffic is in plain text, the attacker can read the traffic when the attacker gains access to the path. An example is an attack performed by controlling a router on the data path.

The default recommendation and setting for traffic within Skype for Business Server is to use mutual TLS (MTLS) between trusted servers and TLS from client to server. This protective measure would make an attack very difficult or impossible to achieve within the time period in which a given conversation occurs. TLS authenticates all parties and encrypts all traffic. This does not prevent eavesdropping, but the attacker cannot read the traffic unless the encryption is broken.

The Traversal Using Relay NAT (TURN) protocol does not mandate the traffic to be encrypted and the information that it is sending is protected by message integrity. Although it is open to eavesdropping, the information it is sending (that is, the IP addresses and port) can be extracted directly by simply looking at the source and destination addresses of the packets. The A/V Edge service ensures that the data is valid by checking the Message Integrity of the message by using the key derived from a few items, including a TURN password, which is never sent in clear text. If Secure Real Time Protocol (SRTP) is used, media traffic is also encrypted.

## Identity Spoofing (IP Address and Caller Id Spoofing)

Identity Spoofing occurs when the attacker determines and uses a phone number of a valid user (caller id) or an IP address of a network, computer, or network component without being authorized to do so. A successful attack allows the attacker to operate as if the attacker is the entity normally identified by the phone number (caller id) or the IP address.

Within the context of Skype for Business Server, IP Address Spoofing comes into play only if an administrator has done both of the following:

- Configured connections that support only Transmission Control Protocol (TCP) (which is not recommended, because TCP communications are unencrypted).
- Marked the IP addresses of those connections as trusted hosts.

This is less of a problem for Transport Layer Security (TLS) connections, as TLS authenticates all parties and encrypts all traffic. Using TLS prevents an attacker from performing IP address spoofing on a specific connection (for example, mutual TLS connections). But an attacker could still spoof the address of the DNS server that Skype for Business Server uses. However, because authentication in Skype for Business is performed with certificates, an attacker would not have a valid certificate required to spoof one of the parties in the communication.

On the other hand, Caller Id Spoofing comes into play when you have established a SIP trunk between a provider, PSTN gateway or another PBX system and Skype for Business Server. In these cases, Skype for Business Server does not offer any protection to prevent against caller id spoofing. This means that a Skype for Business user can receive a call from the SIP trunk with a spoofed caller id displaying the phone number or display name (if reverse number lookup applies) of another Skype for Business user. Protection to this should be applied on the provider side, PSTN or PBX gateway.

## Man-in-the-Middle Attack

A man-in-the-middle attack occurs when an attacker reroutes communication between two users through the attacker's computer without the knowledge of the two communicating users. The attacker can monitor and read the traffic before sending it on to the intended recipient. Each user in the communication unknowingly sends traffic to and receives traffic from the attacker, all while thinking they are communicating only with the intended user. This can happen if an attacker can modify Active Directory Domain Services to add his or her server as a trusted server or modify Domain Name System (DNS) to get clients to connect through the attacker on their way to the server. A man-in-the-middle attack can also occur with media traffic between two clients. However, in Skype for Business Server point-to-point audio, video, and application sharing, streams are encrypted with SRTP, using cryptographic keys that are negotiated between the peers that are using Session Initiation Protocol (SIP) over TLS. Servers such as Group Chat make use of HTTPS to enhance the security of web traffic.

## RTP Replay Attack

A replay attack occurs when a valid media transmission between two parties is intercepted and retransmitted for malicious purposes. SRTP used in connection with a secure signaling protocol protects transmissions from replay attacks by enabling the receiver to maintain an index of already received RTP packets and compare each new packet with those already listed in the index.

# Spim

Spim is unsolicited commercial instant messages or presence subscription requests. While not by itself a compromise of the network, it is annoying in the least, can reduce resource availability and production, and can possibly lead to a compromise of the network. An example of this is users spimming each other by sending requests. Users can block each other to prevent this, but with federation, if a coordinated spim attack is established, this can be difficult to overcome unless you disable federation for the partner.

## Viruses and Worms

A virus is a unit of code whose purpose is to reproduce additional, similar code units. To work, a virus needs a host, such as a file, email, or program. A worm is a unit of code whose purpose is to reproduce additional, similar code units, but it does not need a host. Viruses and worms primarily show up during file transfers between clients or when URLs are sent from other users. If a virus is on your computer, it can, for example, use your identity and send instant messages on your behalf.

## Personally Identifiable Information

Skype for Business Server has the potential to disclose information over a public network that might be able to be linked to an individual. The information types can be broken down to two specific categories:

- **Enhanced presence data** Enhanced presence data is information that a user can choose to share or not share over a link to a federated partner or with contacts within an organization. This data is not shared with users on a public IM network. Client policies and other client configuration may put some control with the system administrator. In Skype for Business Server, enhanced presence privacy mode can be configured for an individual user to prevent Skype for Business users not on the user's Contacts list from seeing the user's presence information. Enhanced presence privacy mode does not prevent users of Microsoft Office Communicator 2007 and Microsoft Office Communicator 2007 R2 from seeing a user's presence information. For details about deploying the client and presence, see [Deploy clients for Skype for Business Server](#) and [Plan for instant messaging and presence in Skype for Business Server](#).
- **Mandatory data** Mandatory data is required for the proper operation of the server or the client and is NOT under the control of the client or system administration. This is information that is necessary at a server or network level for the purposes of routing, state maintenance, and signaling.

The following tables list the data that is exposed over a public network.

### Enhanced Presence Data

DATA DISCLOSED	POSSIBLE SETTINGS
Personal Data	Name, Title, Company, Email Address, Time Zone
Telephone Numbers	Work, Mobile, Home
Calendar Information	Free/Busy, Out-Of-Town Notice, Meeting Details (to those who have access to your calendar)
Presence Status	Away, Available, Busy, Do Not Disturb, Offline

### Mandatory Data



<b>DATA DISCLOSED</b>	<b>EXAMPLE INFORMATION</b>
IP Address	Actual address of computer or NATed address
SIP URI	jeremylos@litwareinc.com

# Security framework for Skype for Business Server

5/20/2019 • 2 minutes to read

This section provides an overview of the fundamental elements that form the security framework for Skype for Business Server. Understanding how these elements work together is essential to making informed decisions about securing your particular Skype for Business Server deployment.

These elements are as follows:

- Active Directory Domain Services (AD DS) provides a single trusted back-end repository for user accounts and network resources.
- Role-Based Access Control (RBAC) enables you to delegate administrative tasks while maintaining high standards for security.
- Public Key Infrastructure (PKI) uses certificates issued by trusted certification authorities (CAs) to authenticate servers and ensure data integrity.
- Transport Layer Security (TLS), HTTPS over SSL (HTTPS), and mutual TLS (MTLS) enable endpoint authentication and IM encryption. Point-to-point audio, video, and application sharing streams are encrypted using Secure Real-Time Transport Protocol (SRTP).
- Industry-standard protocols for user authentication, where possible.
- Windows PowerShell provides security features that are enabled by default so that users cannot easily or unknowingly run scripts.

These fundamental security elements work together to define trusted users, servers, connections, and operations to help ensure a secure foundation for Skype for Business Server.

## In this section

The topics in this section describe how each of these fundamental elements works to enhance the security of your Skype for Business Server infrastructure.

- [Active Directory Domain Services for Skype for Business Server](#)
- [Role-based access control \(RBAC\) for Skype for Business Server](#)
- [Public Key Infrastructure for Skype for Business Server](#)
- [TLS and MTLS for Skype for Business Server](#)
- [Encryption for Skype for Business Server](#)
- [User and client authentication for Skype for Business Server](#)
- [Windows PowerShell and Skype for Business Server management tools](#)

# Active Directory Domain Services for Skype for Business Server

5/20/2019 • 6 minutes to read

Active Directory Domain Services functions as the directory service for Windows Server 2003, Windows Server 2008, Windows Server 2012, and Windows Server 2012 R2 networks. Active Directory Domain Services also serves as the foundation on which the Skype for Business Server security infrastructure is built. The purpose of this section is to describe how Skype for Business Server uses Active Directory Domain Services to create a trustworthy environment for IM, Web conferencing, media, and voice. For details about preparing your environment for Active Directory Domain Services, see [Install Skype for Business Server](#) in the Deployment documentation. For details about the role of Active Directory Domain Services in Windows Server networks, see the documentation for the version of the operating system you are using.

Skype for Business Server uses Active Directory Domain Services to store:

- Global settings that all servers running Skype for Business Server in a forest require.
- Service information that identifies the roles of all servers running Skype for Business Server in a forest.
- Some user settings.

## Active Directory Infrastructure

Infrastructure requirements for Active Directory include the following:

- Operating system requirements for domain controllers
- Domain and forest functional level requirements
- Global catalog domain requirements

For details, see [Environmental requirements for Skype for Business Server 2015](#) or [Server requirements for Skype for Business Server 2019](#).

## Universal Groups

During preparation of the forest, Skype for Business Server creates various universal groups within Active Directory Domain Services that have permission to access and manage global settings and services. These universal groups include:

- **Administrative groups.** These groups define the fundamental administrator roles for a Skype for Business Server network. During forest preparation, these administrator groups are added to Skype for Business Server infrastructure groups.
- **Service groups.** These groups are service accounts that are required to access various services provided by Skype for Business Server.
- **Infrastructure groups.** These groups provide permission to access specific areas of the Skype for Business Server infrastructure. They function as components of administrative groups, and you should not modify them or add users to them directly. During forest preparation, specific service and administration groups are added to the appropriate infrastructure groups.

For details about the specific universal groups created when preparing AD for Skype for Business Server, as well

as the service and administration groups that get added to the infrastructure groups, see [Changes made by forest preparation in Skype for Business Server](#) in the Deployment documentation.

#### NOTE

Skype for Business Server supports the universal groups in the Windows Server 2012, as well as Windows Server 2003 operating systems for domain controllers. Members of universal groups can include other groups and accounts from any domain in the domain tree or forest and can be assigned permissions in any domain in the domain tree or forest. Universal group support, combined with administrator delegation, simplifies the management of a Skype for Business Server deployment. For example, it is not necessary to add one domain to another to enable an administrator to manage both.

## Role-Based Access Control

In addition to creating universal service and administration groups and adding service and administration groups to the appropriate universal groups, forest preparation also creates Role-Based Access Control (RBAC) groups. For details about the specific RBAC groups created by forest preparation, see [Changes made by forest preparation in Skype for Business Server](#) in the Deployment documentation. For more information about RBAC groups, see [Role-based access control \(RBAC\) for Skype for Business Server](#).

## Access Control Entries (ACEs) and Inheritance

Forest preparation creates both private and public ACEs and, adding ACEs for the universal groups it creates. It creates specific private ACEs on the global settings container used by Skype for Business Server. This container is used only by Skype for Business Server and is located either in the Configuration container or the System container in the root domain, depending on where you store global settings.

The domain preparation step adds the necessary access control entries (ACEs) to universal groups that grant permissions to host and manage users within the domain. Domain preparation creates ACEs on the domain root and three built-in containers: User, Computers, and Domain Controllers.

For details about the public ACEs created and added by forest preparation and domain preparation, see [Changes made by forest preparation in Skype for Business Server](#) and [Changes made by domain preparation in Skype for Business Server](#) in the Deployment documentation.

Organizations often lock down Active Directory Domain Services (AD DS) to help mitigate security risks. However, a locked-down Active Directory environment can limit the permissions that Skype for Business Server requires. This can include removal of ACEs from containers and OUs and disabling of permissions inheritance on User, Contact, InetOrgPerson, or Computer objects. In a locked down Active Directory environment, permissions must be set manually on containers and OUs that require them.

## Server Information

During activation, Skype for Business Server publishes server information to the three following locations in Active Directory Domain Services:

- A service connection point (SCP) on each Active Directory computer object corresponding to a physical computer on which Skype for Business Server is installed.
- Server objects created in the container of the **msRTCSIP-Pools** class.
- Trusted servers specified in Topology Builder.

## Service Connection Points

Each Skype for Business Server object in Active Directory Domain Services has an SCP called RTC Services, which

in turn contains a number of attributes that identify each computer and specify the services that it provides. Among the more important SCP attributes are *serviceDNSName* , *serviceDNSNameType* , *serviceClassname* , and *serviceBindingInformation* . Third-party asset management applications can retrieve server information across a deployment by querying against these and other SCP attributes.

## Active Directory Server Objects

Each Skype for Business Server server role has a corresponding Active Directory object whose attributes define the services provided by that role. Also, when a Standard Edition server is activated, or when an Enterprise Edition pool is created, Skype for Business Server creates a new **msRTCSIP-Pool** object in the **msRTCSIP-Pools** container. The **msRTCSIP-Pool** class specifies the fully qualified domain name (FQDN) of the pool, along with the association between the front-end and back-end components of the pool. (A Standard Edition server is regarded as a logical pool whose front and back ends are collocated on a single computer.)

## Trusted Servers

In Skype for Business Server, trusted servers are the ones specified when you run Topology Builder and publish your topology. The published topology, including all the server information, is stored in the Central Management store. Only servers defined in the Central Management store are trusted. In Skype for Business Server, a trusted server is one that meets the following criteria:

- The FQDN of the server occurs in the topology stored in Central Management store.
- The server presents a valid certificate from a trusted CA. For details, see [Environmental requirements for Skype for Business Server 2015](#) or [System requirements for Skype for Business Server 2019](#).

If either of these criteria is missing, the server is not trusted and connection with it is refused. This double requirement prevents a possible, if unlikely, attack in which a rogue server attempts to take over a valid server's FQDN.

Additionally, to enable Microsoft Office Communications Server 2007 R2 and Microsoft Office Communications Server 2007 deployments to communicate with Skype for Business Server servers, Skype for Business Server creates containers during forest preparation for holding lists of trusted servers for previous releases. The following table describes the containers created to enable compatibility with previous deployments.

### Trusted Server Lists and Their Active Directory Containers for Compatibility with Previous Releases

TRUSTED SERVER LIST	ACTIVE DIRECTORY CONTAINER
Standard Edition servers and Enterprise pool Front End Servers	RTC Service/Global Settings
Conferencing Servers	RTC Service/Trusted MCUs
Web Components Servers	RTC Service/TrustedWebComponentsServers
Mediation Servers and Communicator Web Access Servers, Application Server, Registrar with QoE, A/V Conferencing Service (also 3rd-party SIP servers)	RTC Service/Trusted Services
Proxy Servers	Skype for Business Server does not support backward compatibility for proxy servers

See also

Prepare Active Directory for Skype for Business Server

# Role-based access control (RBAC) for Skype for Business Server

7/17/2019 • 2 minutes to read

Skype for Business Server includes Role-Based Access Control (RBAC) groups to enable you to delegate administrative tasks while maintaining high standards for security. These groups are created during forest preparation. For details about forest preparation, see [Active Directory Domain Services for Skype for Business Server](#). For details about the specific groups created by forest preparation, see [Changes made by forest preparation in Skype for Business Server](#) in the Deployment documentation.

With RBAC, administrative privilege is granted by assigning users to pre-defined administrative roles, including the 11 predefined roles that cover many common administrative tasks. Each role is associated with a specific list of Skype for Business Server Management Shell cmdlets that users in that role are allowed to run. You can use RBAC to follow the principle of "least privilege," in which users are given only the administrative abilities that their jobs require.

More details on RBAC roles can be found at [Planning for role-based access control](#).

# Public Key Infrastructure for Skype for Business Server

5/20/2019 • 2 minutes to read

Skype for Business Server relies on certificates for server authentication and to establish a chain of trust between clients and servers and among the different server roles. The Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 Public Key Infrastructure (PKI) provides the infrastructure for establishing and validating this chain of trust.

Certificates are digital IDs. They identify a server by name and specify its properties. To ensure that the information on a certificate is valid, the certificate must be issued by a CA that is trusted by clients or other servers that connect to the server. If the server connects only with other clients and servers on a private network, the CA can be an enterprise CA. If the server interacts with entities outside the private network, a public CA might be required.

Even if the information on the certificate is valid, there must be some way to verify that the server presenting the certificate is actually the one represented by the certificate. This is where the Windows PKI comes in.

Each certificate is linked to a public key. The server named on the certificate holds a corresponding private key that only it knows. A connecting client or server uses the public key to encrypt a random piece of information and sends it to the server. If the server decrypts the information and returns it as plain text, the connecting entity can be sure that the server holds the private key to the certificate and therefore is the server named on the certificate.

## NOTE

Not all public CAs comply with the requirements of Skype for Business Server certificates. We recommend that you refer to the listing of certified Public CA vendors for your public certificate needs. For details, see [Unified Communications Certificate Partners](#).

## CRL Distribution Points

Skype for Business Server requires all server certificates to contain one or more Certificate Revocation List (CRL) distribution points. CRL distribution points (CDPs) are locations from which CRLs can be downloaded for purposes of verifying that the certificate has not been revoked since the time it was issued and the certificate is still within the validity period. A CRL distribution point is noted in the properties of the certificate as a URL, and is typically secure HTTP.

## Enhanced Key Usage

Skype for Business Server requires all server certificates to support Enhanced Key Usage (EKU) for the purpose of server authentication. Configuring the EKU field for server authentication means that the certificate is valid for the purpose of authenticating servers. This EKU is essential for MTLS. It is possible to have more than one entry in the EKU, enabling the certificate for more than one purpose.



# TLS and MTLs for Skype for Business Server

5/20/2019 • 2 minutes to read

Transport Layer Security (TLS) and Mutual Transport Layer Security (MTLS) protocols provide encrypted communications and endpoint authentication on the Internet. Skype for Business Server uses these two protocols to create the network of trusted servers and to ensure that all communications over that network are encrypted. All SIP communications between servers occur over MTLS. SIP communications from client to server occur over TLS.

TLS enables users, through their client software, to authenticate the Skype for Business Server servers to which they connect. On a TLS connection, the client requests a valid certificate from the server. To be valid, the certificate must have been issued by a CA that is also trusted by the client and the DNS name of the server must match the DNS name on the certificate. If the certificate is valid, the client uses the public key in the certificate to encrypt the symmetric encryption keys to be used for the communication, so only the original owner of the certificate can use its private key to decrypt the contents of the communication. The resulting connection is trusted and from that point is not challenged by other trusted servers or clients. Within this context, Secure Sockets Layer (SSL) as used with Web services can be associated as TLS-based.

Server-to-server connections rely on MTLS for mutual authentication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other. In Skype for Business Server deployments, certificates issued by the enterprise CA that are during their validity period and not revoked by the issuing CA are automatically considered valid by all internal clients and servers because all members of an Active Directory domain trust the Enterprise CA in that domain. In federated scenarios, the issuing CA must be trusted by both federated partners. Each partner can use a different CA, if desired, so long as that CA is also trusted by the other partner. This trust is most easily accomplished by the Edge Servers having the partner's root CA certificate in their trusted root CAs, or by use of a third-party CA that is trusted by both parties.

TLS and MTLS help prevent both eavesdropping and man-in-the-middle attacks. In a man-in-the-middle attack, the attacker reroutes communications between two network entities through the attacker's computer without the knowledge of either party. TLS and Skype for Business Server specification of trusted servers (only those specified in Topology Builder) mitigate the risk of a man-in-the-middle attack partially on the application layer by using end-to-end encryption coordinated using the Public Key cryptography between the two endpoints, and an attacker would have to have a valid and trusted certificate with the corresponding private key and issued to the name of the service to which the client is communicating to decrypt the communication. Ultimately, however, you must follow best security practices with your networking infrastructure (in this case corporate DNS). Skype for Business Server assumes that the DNS server is trusted in the same way that domain controllers and global catalogs are trusted, but DNS does provide a level of safeguard against DNS hijack attacks by preventing an attacker's server from responding successfully to a request to the spoofed name.

# Encryption for Skype for Business Server

5/20/2019 • 2 minutes to read

Skype for Business Server uses TLS and MTLS to encrypt instant messages. All server-to-server traffic requires MTLS, regardless of whether the traffic is confined to the internal network or crosses the internal network perimeter. When connecting Skype for Business Server to third-party IPPBX systems or SIP trunks TLS is optional but strongly recommended between the Mediation Server and media gateway. If TLS is configured on this link, MTLS is required. Therefore, the gateway must be configured with a certificate from a CA that is trusted by the Mediation Server.

## NOTE

A security advisory regarding SSL 3.0 was published in 2014. Disabling SSL 3.0 in Skype for Business Server 2015 is a supported option. To learn more about the security advisory, see [Disabling SSL 3.0 in Lync Server 2013 and Skype for Business Server 2015](#).

**Security note:** To ensure the strongest cryptographic protocol is used, Skype for Business Server 2015 will offer TLS encryption protocols in the following order to clients: **TLS 1.2**, **TLS 1.1**, **TLS 1.0**. TLS is a critical aspect of Skype for Business Server 2015 and thus it is required in order to maintain a supported environment.

**Security note:** To ensure the strongest cryptographic protocol is used, Skype for Business Server 2019 will offer TLS encryption protocols in the following order to clients: **TLS 1.3**, **TLS 1.2**. TLS is a critical aspect of Skype for Business Server 2019 and thus it is required in order to maintain a supported environment.

The following table summarizes the protocol requirements for each type of traffic.

## Traffic Protection

TRAFFIC TYPE	PROTECTED BY
Server-to-server	MTLS
Client-to-server	TLS
Instant messaging and presence	TLS
Audio and video and desktop sharing of media	SRTP
Desktop sharing (signaling)	TLS
Web conferencing	TLS
Meeting content download, address book download, distribution group expansion	HTTPS

## Media Encryption

Media traffic is encrypted using Secure RTP (SRTP), a profile of Real-Time Transport Protocol (RTP) that provides confidentiality, authentication, and replay attack protection to RTP traffic. In addition, media flowing in both directions between the Mediation Server and its internal next hop is also encrypted using SRTP. Media flowing in both directions between the Mediation Server and a media gateway is optionally encrypted and recommended. The Mediation Server can support encryption to the media gateway, but the gateway must support MTLS and

storage of a certificate.

**NOTE**

For more information about setting up hybrid, see [Plan hybrid connectivity](#).

## FIPS

Skype for Business Server and Microsoft Exchange Server 2016 operate with support for Federal Information Processing Standard (FIPS) 140-2 algorithms if the Windows Server operating systems are configured to use the FIPS 140-2 algorithms for system cryptography. To implement FIPS support, you must configure each server running Skype for Business Server to support it.

# Windows PowerShell and Skype for Business Server management tools

5/20/2019 • 2 minutes to read

In Skype for Business Server, management tools are implemented using Windows PowerShell. Windows PowerShell includes a command-line environment, product-specific commands, and a full scripting language. Skype for Business Server tools that are implemented using Windows PowerShell include the following:

- **Topology Builder.** You use Topology Builder to create, adjust, and publish your planned topology, and it validates your topology before you begin server installations. When you install Skype for Business Server on individual servers, the servers read the published topology as part of the installation process, and the installation program deploys the server as directed in the topology. After setup, configuration information is automatically replicated to all servers. Components can be added to your deployment only by using Topology Builder.
- **Skype for Business Server Management Shell.** You can use Skype for Business Server Management Shell for full command-line management of your deployment.
- **Skype for Business Server Control Panel.** You can use the Skype for Business Server Control Panel user interface to manage the most common tasks in your deployment.

These tools use Windows PowerShell cmdlets for management of your deployment, including close to 550 product-specific cmdlets. The security cmdlets included in Skype for Business Server are primarily used to manage authentication, and user rights and permissions. A wide variety of cmdlets are available for managing authentication, including cmdlets for certificate and personal identification number (PIN) authentication. In addition, a number of cmdlets enable you to use the new Role-Based Access Control (RBAC) feature to delegate administrative control of Skype for Business Server. For details about the Skype for Business Server cmdlets, see [Skype for Business Server Management Shell](#).

The script security features for Windows PowerShell are specifically designed to help prevent some of the scripting-related security problems of older technologies, including Microsoft Visual Basic Scripting Edition (VBScript). The Windows PowerShell security features are intended to create an environment in which users cannot easily or unknowingly run scripts. By default, Windows PowerShell security features are enabled. You can modify the state of those features to accommodate your scripting needs and a variety of security goals. This is not to say that the shell makes it impossible for users to run scripts. Rather, the shell makes it difficult—by default—for users to run scripts without realizing they are doing so. For details, see [Windows PowerShell Script Security](#).

# Addressing threats to your core infrastructure for Skype for Business Server

5/20/2019 • 2 minutes to read

In addition to following best practices for your Skype for Business Server deployment, you can help to ensure security by reviewing, understanding, and addressing any needs in specific areas of your deployment.

## In this section

- [Best practices for your core infrastructure in Skype for Business Server](#)

# Capacity planning for Skype for Business Server

5/20/2019 • 2 minutes to read

The topics in this section help you understand how to plan and deploy Skype for Business Server so that you can adequately plan for the number of users in your organization and plan for the server load that their activities generate.

## NOTE

All recommendations in this section assume that you have installed Skype for Business Cumulative Update, November 2015, or later, on your servers.

## In this section

- [Capacity planning user model usage for Skype for Business Server](#)
- [Estimating voice usage and traffic for Skype for Business Server](#)
- [Deployment guidelines for Mediation Server in Skype for Business Server](#)
- [User models in Skype for Business Server](#)

# Capacity Planning for Skype for Business Server 2019

5/20/2019 • 13 minutes to read

This article provides guidance on how many servers you need at a site for the number of users at that site, according to the usage described in [User models in Skype for Business Server](#)

## Tested Hardware Platform

We've done our performance testing on the hardware described in the table below. All our recommendations and results are based on this hardware. If you decide to try using less powerful hardware than what you see listed here, please be aware that you may face functionality problems or poor performance.

### Hardware Used in Performance Testing

HARDWARE COMPONENT	RECOMMENDED
CPU	Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher. Intel Itanium processors are not supported for Skype for Business Server 2019 roles.
Memory	32 gigabytes (GB).
Disk	EITHER: • 8 or more 10000 RPM hard disk drives with at least 72 GB free disk space (two of the disks using RAID 1 and 6 using RAID 10). OR • Solid state drives (SSDs) able to provide the same free space and similar performance to 8 10000 RPM mechanical disk drives.
Network	1 dual-port network adapter, 1 Gbps or higher (2 network adapters can be used, but they need to be teamed with a single MAC address and a single IP address). Dual or multi-homed configurations are <b>not</b> supported for Front End Servers, Back End Servers, and Standard Edition servers. As long as they are not exposed to the operating system and are being used to monitor and manage server hardware, you can have out-of-band management systems, such as DRAC or ILO. This scenario doesn't constitute a multi-homed server, and it is supported.

## Summary of Results

The following table summarizes our recommendations.

SERVER ROLE	MAXIMUM NUMBER OF USERS SUPPORTED
-------------	-----------------------------------

SERVER ROLE	MAXIMUM NUMBER OF USERS SUPPORTED
Front End pool with sixteen Front End Servers and Back End Server or a pair of Back End Servers with SQL Always On for High Availability.	106,000 unique users simultaneously logged in, plus 50% multiple points of presence (MPOP) representing non-mobile instances, plus 40% of users enabled for Mobility for a total of 210,000 endpoints.
A/V Conferencing	<p>The A/V Conferencing service provided by a Front End pool supports the pool's conferences assuming a maximum conference size of 250 users, and only one such large conference running at a time.</p> <p><b>Note:</b> Additionally, you can support large conferences of between 250 and 1000 users by deploying a separate Front End pool with two Front End Servers to host the large conferences. For details, see <a href="#">Plan for large meetings in Skype for Business Server</a>.</p>
One Edge Server	18,000 concurrent remote users.
One Director	18,000 concurrent remote users.
Monitoring and Archiving	<p>The Monitoring and Archiving front end services run on each Front End Server, instead of on separate server roles. Monitoring and Archiving each still require their own database stores. If you also run Exchange 2013 or later, you can keep your Archiving data in Exchange, rather than in a dedicated SQL database.</p>
One Mediation Server	Mediation Server collocated with Front End Server runs on every Front End Server in a pool, and should provide enough capacity for the users in the pool. For stand-alone Mediation Server, see the "Mediation Server" section later in this topic.
One Standard Edition server	<p>We strongly recommend that if you use Standard Edition servers to host users, you always use two servers, paired using the recommendations in <a href="#">Planning for High Availability and Disaster Recovery</a>. Each server in the pair can host up to 2,500 users, and if one server fails the remaining server can support 5,000 users in a failover scenario.</p> <p>If your deployment includes a significant amount of audio or video traffic, server performance may suffer with more than 2,500 users per server. In this case, you should consider adding more Standard Edition servers or moving to Skype for Business Server Enterprise Edition.</p>

## Front End Server

### NOTE

Stretched pools aren't supported for this server role.

In a Front End pool, you should have one Front End Server for every 6,660 users homed in your pool, assuming that hyper-threading is enabled on all servers in the pool, that you are using SQL Server Express Edition, and that the server hardware meets the recommendations in [Server requirements for Skype for Business Server 2019](#). The maximum number of users in one Front End pool is 106,000, again assuming that hyper-threading is enabled and SQL Server Express Edition is used on all the servers in your pool. If you have more than 106,000 users at a site, you can deploy more than one Front End pool.



When you account for the number of users in a Front End pool, include any users homed on Survivable Branch Appliances and Survivable Branch Servers at branch offices that are associated with this Front End pool.

When an active server is unavailable, its connections are transferred automatically to the other servers in the pool. In a scenario where you have 30,000 users and five Front End Servers, if one server is unavailable, the connections of 6000 of your users need to be transferred to your other four remaining servers. These four remaining servers will then each have 7500 users, which is a larger number than recommended.

If instead you had started with six Front End Servers for your 30,000 users and one becomes unavailable, a total of 5000 users need to move to the remaining five servers. These five remaining servers will then each host 6000 users, which is in the recommended range.

The maximum number of users in a Front End pool is 106,000. The maximum number of Front End Servers in a pool is 16.

For a Front End pool with 80,000 users, 16 Front End Servers will be good for performance, in typical deployments that follow the [User models in Skype for Business Server](#). Deployments designed to support disaster recovery failover assume that a maximum of 53,000 users can be hosted in each of two paired Front End pools, in which each pool has enough Front End Servers to contain the users in both pools, should one pool need to be failed over to the other.

The number of users supported with good performance by a particular Front End pool may differ from these numbers for the following reasons:

- The hardware for your Front End Servers doesn't meet the recommendations.
- Instead of using SQL Server Express Edition, you use another SQL Server Edition, you may be able to host additional users in each Front End pool.
- Your organization's usage is very different from the user models, for example, if you have a lot more conferencing traffic.

The following table shows the average bandwidth for IM and presence, given the user model, as defined in [User models in Skype for Business Server](#).

AVERAGE BANDWIDTH PER USER	BANDWIDTH REQUIREMENTS PER FRONT END SERVER WITH 6,660 USERS
3-3.75 KBps	13 MBps

#### NOTE

To improve the media performance of the co-located A/V Conferencing and Mediation Server functionality on your Front End Servers, you should enable receive-side scaling (RSS) on the network adapters on your Front End Servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see [Receive Side Scaling \(RSS\) in the Windows Server 2012 documentation](#). For details about how to enable RSS, you'll need to refer to your network adapter documentation.

## Conferencing Maximums

Given the user model that 5% of users in a pool may be in a conference at any one time, a pool of 106,000 users could have about 5,300 users in conferences simultaneously. These conferences are expected to be a mix of media (some IM-only, some IM with audio, some audio/video, for example) and number of participants. There isn't a hard limit for the actual number of conferences allowed, and actual usage determines the actual performance. For example, if your organization has many more mixed-mode conferences than are assumed in the user model, you might need to deploy more Front End Servers or A/V Conferencing Servers than the recommendations found in this article. For details about the assumptions in the user model, see [User models in Skype for Business Server](#).

The maximum supported conference size hosted by a regular Skype for Business Server Front End pool which also hosts users is 250 participants. While a 250-user conference is happening, the pool still supports other conferences as well, such that a total of 5% of pool users are in concurrent conferences. For example, in a pool of 16 Front End Servers and 106,000 users, while the 250-user conference is happening, Skype for Business Server supports 5,050 other users participating in smaller conferences.

Regardless of the number of users homed on the Front End pool or Standard Edition server, Skype for Business Server supports a minimum of 125 other users participating in smaller conferences on the same pool or server which is hosting a 250-user conference.

To enable conferences that have between 250 and 1000 users, you can set up a separate Front End pool just to host those conferences. This Front End pool won't host any users. For details, please see [Plan for large meetings in Skype for Business Server](#).

If your organization has a lot more mixed-mode conferences than are assumed in the user model, you might need to deploy more Front End Servers than we recommendation in this document (up to a limit of 16 Front End Servers). For details about the assumptions in the user model, see [User models in Skype for Business Server](#).

## Edge Server

### NOTE

Stretched pools aren't supported for this server role.

You should deploy one Edge Server for every 18,000 remote users who will access a site concurrently. At a minimum we recommend two Edge Servers for high availability. These recommendations assume that the hardware for your Edge Servers meets the recommendations in [Server Hardware Platforms](#).

When you account for the number of users for the Edge Servers, include the users homed on Survivable Branch Appliances and Survivable Branch Servers at branch offices that are associated with a Front End pool at this site.

### NOTE

To improve the performance of the A/V Conferencing Edge service on your Edge Servers, you should enable receive-side scaling (RSS) on the network adapters on your Edge Servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, check [Receive Side Scaling \(RSS\) in Windows Server 2012](#). For details about how to enable RSS, you'll need to refer to your network adapter documentation.

## Director

### NOTE

Stretched pools aren't supported for this server role.

If you deploy the Director server role, we recommend that you deploy one Director for every 18,000 remote users who will access a site concurrently. At a minimum we recommend two Directors for high availability. These recommendations assume that the hardware for your Edge Servers meets the recommendations in [Server Hardware Platforms](#).

When you account for the number of users for the Directors, include the users homed on Survivable Branch Appliances and Survivable Branch Servers at branch offices that are associated with a Front End pool at this site.

## Mediation Server

**NOTE**

Stretched pools aren't supported for this server role.

If you collocate Mediation Server with Front End Server, Mediation Server runs on every Front End Server in the pool, and should provide enough capacity for the users in the pool.

If you deploy a stand-alone Mediation Server pool, then how many Mediation Servers to deploy depends on many factors, including the hardware used for Mediation Server, the number of VoIP users you have, the number of gateway peers that each Mediation Server pool controls, the busy hour traffic through those gateways, and the percentage of calls with media that bypasses the Mediation Server.

The following tables provide a guideline for how many concurrent calls a Mediation Server can handle, assuming that the hardware for the Mediation Servers meets the requirements in [Server Hardware Platforms](#) and that hyper-threading is enabled. For details about Mediation Server scalability, see [Estimating voice usage and traffic for Skype for Business Server](#) and [Deployment guidelines for Mediation Server in Skype for Business Server](#).

All the following tables assume usage as summarized in [User models in Skype for Business Server](#).

**Stand-alone Mediation Server Capacity: 70% Internal Users, 30% External users with non-bypass call capacity (media transcoding performed by Mediation Server)**

SERVER HARDWARE	MAXIMUM NUMBER OF CALLS	MAXIMUM NUMBER OF T1 LINES	MAXIMUM NUMBER OF E1 LINES
Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher <b>with hyper-threading disabled</b> , with 64 GB memory and one dual-port network adapter card.	1500	64	49
Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher, with 64 GB memory and one dual-port network adapter card.	2000	88	66

**NOTE**

Although servers with 64 GB of memory were used for performance testing, servers with 32 GB of memory are supported for stand-alone Mediation Server, and are sufficient to provide the performance shown in this table.

**Mediation Server Capacity (Mediation Server Collocated with Front End Server) 70% Internal Users, 30% External Users, Non-Bypass Call Capacity (Media Processing Performed by Mediation Server)**

SERVER HARDWARE	MAXIMUM NUMBER OF CALLS
Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher, with 64 GB memory and 2 1GB network adapter cards.	200

**NOTE**

This number is much smaller than the numbers for the stand-alone Mediation Server. That's because the Front End Server has to handle other features and functions for the 6600 users homed on it, in addition to the transcoding needed for voice calls.

**NOTE**

To improve the performance of the Mediation Server, you should enable receive-side scaling (RSS) on the network adapters on your Mediation Servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "[Receive-Side Scaling in Windows Server 2012](#)". For details about how to enable RSS, you'll need to refer to your network adapter documentation.

## Back End Server

Although much of the database information is stored primarily on the Front End Servers, you should make sure your Back End Servers meet the hardware recommendations listed earlier in this section and in [Server Hardware Platforms](#).

To provide high availability of your Back End Server, we recommend deploying AlwaysOn Availability Groups or server mirroring. For more information, see [Back End Server high availability in Skype for Business Server](#).

## Monitoring and Archiving

If you deploy Monitoring or Archiving, the front end functionality of these services runs on the Front End Servers, Monitoring and Archiving each use their own database store, separate from the Back End store. Alternatively, if you have Exchange 2013 deployed, you can store instant message Archiving data in Exchange instead of in a dedicated SQL store.

The following table indicates approximately how much database storage is required per user per day for Monitoring and Archiving data.

	CDR (MONITORING)	QOE (MONITORING)	ARCHIVING
Disk space required per user per day	49 KB	28 KB	57 KB

Microsoft used the hardware in the following table for the database server for Monitoring and Archiving during its performance testing. The testing collected the data of two Front End pools, each of which contained 80,000 users.

### Hardware Used in Monitoring and Archiving Performance Testing

HARDWARE COMPONENT	RECOMMENDED
CPU	Intel Xeon E5-2673 v3 dual processor, 6-core, 2.4 gigahertz (GHz) or higher.
Memory	48 GB

HARDWARE COMPONENT	RECOMMENDED
Disk	<p>EITHER:</p> <ul style="list-style-type: none"> <li>• 4 or more 10000 RPM hard disk drives with at least 72 GB free disk space (the disks should be in a 2x RAID 1 configuration).</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• Solid state drives (SSDs) able to provide the same free space and similar performance to 4 10000 RPM mechanical disk drives.</li> </ul>
Network	1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and single IP address).

### Recommended Disk configurations

DRIVE	RAID CONFIGURATION	NUMBER OF DISKS
CDR, QoE, and Archiving database data files, on a single drive	1+0	16
CDR database log file	1	2
QoE database log file	1	2
Archiving database log file	1	2

## Video Interop Server capacity

If you deploy Video Interop Server and you need to determine capacity, you look at the maximum number of Video Teleconferencing Systems (VTCs) that will be in concurrent calls. For example, if you have 250 VTCs in your organization and your user model estimates that at most, 20% of them might be in concurrent calls, you base your capacity planning on 50 concurrent VTCs.

# Estimating voice usage and traffic for Skype for Business Server

5/20/2019 • 2 minutes to read

You can use the following metric to estimate user traffic at each site and the number of ports that are required to support that traffic.

For **Light traffic** (one PSTN call per user per hour), figure 15 users per port.

For **Medium traffic** (2 PSTN calls per user per hour), figure 10 users per port.

For **Heavy traffic** (3 or more PSTN per user calls per hour), figure 5 users per port.

The number of ports in turn determines the number of Mediation Servers and gateways that will be required. The public switched telephone network (PSTN) gateways that most organizations consider deploying range in size from 2 ports to as many as 960 ports. (There are even larger gateways, but these are used mainly by telephony service providers.)

For example, an organization with 10,000 users and medium traffic would require 1000 ports. The number of gateways required would equal the total number of ports required as determined by the total capacity of the gateways.

# Deployment guidelines for Mediation Server in Skype for Business Server

5/20/2019 • 3 minutes to read

This topic describes planning guidelines for Mediation Server deployment.

## Collocated or Stand-alone Mediation Server?

Mediation Server is, by default, collocated on the Standard Edition server or Front End Server in a Front End pool at central sites. The number of public switched telephone network (PSTN) calls that can be handled and the number of machines required in the pool will depend on:

- The number of gateway peers that the Mediation Server pool controls.
- The high-volume traffic periods through those gateways.
- The percentage of calls that are calls whose media bypass the Mediation Server.

When you're planning, be sure to take into account the media processing requirements for PSTN calls and A/V conferences that don't support media bypass, as well as the processing needed to handle signaling interactions for the number of busy-hour calls that need to be supported. If you don't have enough CPU, you'll need to deploy a stand-alone pool of Mediation Servers. Additionally, PSTN gateways, IP-PBXs, and SBCs will need to be split into subsets that are controlled by the collocated Mediation Servers in one pool and the stand-alone Mediation Servers in one or more stand-alone pools.

If you deployed PSTN gateways, IP-PBXs, or Session Border Controllers (SBCs) that lack the ability to interact with a pool of Mediation Servers, they'll need to be associated with a stand-alone pool consisting of a single Mediation Server. Some of the things your PSTN gateways, IP-PBXs or SBCs would need to do include:

- Perform network layer Domain Name System (DNS) load balancing across Mediation Servers in a pool (or otherwise route traffic uniformly to all Mediation Servers in a pool).
- Accept traffic from any Mediation Server in a pool.

You can use the Skype for Business Planning Tool to evaluate whether collocating the Mediation Server with your Front End pool can handle the load. If your environment can't meet these requirements, then you'll need to deploy a stand-alone Mediation Server pool.

## Central Site and Branch Site Considerations

Mediation Servers at the central site can be used to route calls for IP-PBXs or PSTN gateways at branch sites. If you deploy SIP trunks, however, you have to deploy a Mediation Server at the site where each trunk terminates. Having a Mediation Server at the central site route calls for an IP-PBX or PSTN gateway at a branch site doesn't require the use of media bypass, but a media bypass is recommended. That's because, if you can enable media bypass, it'll reduce media path latency and, consequently, result in improved media quality because the media path isn't required to follow the signaling path. Media bypass will also decrease the processing load on the pool.

**NOTE**

Media bypass won't interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on Unified Communications Open Interoperability Program - Lync Server at [Explore tested devices, infrastructure, and tools that support and extend your Skype for Business experience](#).

If branch site resiliency is required, a Survivable Branch Appliance or combination of a Front End Server, a Mediation Server, and a gateway must be deployed at the branch site. (The assumption with branch site resiliency is that presence and conferencing are not resilient at the site.) For guidance on branch site planning for voice, see [Plan for Enterprise Voice resiliency in Skype for Business Server](#).

For interactions with an IP-PBX, if the IP-PBX does not correctly support early media interactions with multiple early dialogs and RFC 3960 interactions, there can be clipping of the first few words of the greeting for incoming calls from the IP-PBX to Lync endpoints. This behavior can be more severe if a Mediation Server at a central site is routing calls for an IP-PBX where the route terminates at a branch site, because more time is needed for signaling to complete. If you experience this behavior, deploying a Mediation Server at the branch site is the only way to reduce clipping of the first few words.

Finally, if your central site has a TDM PBX, or if your IP-PBX does not eliminate the need for a PSTN gateway, then you must deploy a gateway on the call route connecting Mediation Server and the PBX.

**NOTE**

To improve the media performance of standalone Mediation Server, you should enable receive-side scaling (RSS) on the network adapters on these servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "[Receive-Side Scaling Enhancements in Windows Server](#)". For details about how to enable RSS, see your network adapter documentation.



# User models in Skype for Business Server

5/20/2019 • 11 minutes to read

The user models described here provide the basis for the capacity planning measurements and recommendations described in [Capacity planning user model usage for Skype for Business Server](#).

## Skype for Business Server User Models

The following table describes the user model for registration, contacts, instant messaging (IM), and presence for Skype for Business Server.

### Environment and Registration User Model

CATEGORY	DESCRIPTION
Deployment size and distribution	We model a large deployment with three central sites, with one Front End pool per site.
Percentage of Active Directory users	We assume that 70% of all Active Directory users in the organization are enabled for Skype for Business Server. 80% of those enabled users are logged on to Skype for Business Server each day (80% concurrency). The concurrent users are the basis for the numbers in the rest of this section.
Active Directory changes	We assume that 0.5% of total users are created and enabled for Skype for Business in Active Directory each week, and that 0.5% of total users are disabled from Active Directory and from Skype for Business each week. 5% of users have at least one Active Directory attribute changed each week.
Active Directory distribution groups	We assume that the number of Active Directory distribution groups in the organization is equal to three times the number of all users in Active Directory. The distribution groups have the following sizes: <ul style="list-style-type: none"><li>• 64% have 2-30 users</li><li>• 13% have 31-50 users</li><li>• 10% have 51-100 users</li><li>• 13% have 101-500 users</li></ul>
Voice over IP (VoIP) users	60% of Skype for Business Server users are enabled for unified communications (UC) (that is, their phone numbers are owned by Skype for Business Server).
Registered client distribution	65% of clients run Skype for Business software, including Skype for Business and Lync Phone Edition. 30% of clients running client software from a previous version of Lync. 5% of clients using Skype for Business Web App. If mobility is enabled, we assume that 40% of users are using mobility concurrently with the other previously cited registered client options. In this case the client multiple point of presence (MPOP) ratio is 1:1.9. If mobility is disabled, the MPOP ratio is 1:1.5.

CATEGORY	DESCRIPTION
Remote user distribution	70% of users connecting internally. 30% of users connecting through an Edge Server (you may also optionally have a Director here, but it's not required).
Contact distribution	The maximum number of contacts a user has is 1,000. Less than 1% of users have 1,000 contacts. Less than 25% of users have 100 or more contacts. Average of 80 contacts for users with public cloud connectivity. Of these users: <ul style="list-style-type: none"> <li>• 50% of the contacts are within the organization. 10% of those users are remote users, connecting from outside the firewall.</li> <li>• 40% of the contacts are Skype users.</li> <li>• 10% of the contacts are from federated partners.</li> </ul> Average of 50 contacts for users without public cloud connectivity. Of these users: <ul style="list-style-type: none"> <li>• 80% of the contacts are within the organization. 10% of those users are remote users, connecting from outside the firewall.</li> <li>• 20% of the contacts are from federated partners.</li> </ul> Each user has 1 distribution group in their contact list. For performance testing, we assume that distribution groups are always expanded.
Session time	The average user logon session lasts 12 hours. All users log on within 120 minutes of the start of the session.

### IM and Presence User Model

CATEGORY	DESCRIPTION
Peer-to-peer IM sessions	Each user averages six peer-to-peer IM sessions per day. 10 instant messages per session. Each message is matched by two SIP INFO messages and 2 SIP 200 OK messages (for the status indicators such as "<Name> is Typing")
Group IM sessions	Average number of messages sent in a group IM-only session is 5 per user. Average number of messages sent in the IM portion of an AV conference is 2 per user.

CATEGORY	DESCRIPTION
Presence polling	<p>Overall, we assume presence polling at an average of 60 polls per user per hour. For each user, assume an average of:</p> <ul style="list-style-type: none"> <li>• One poll per day of the presence of users in the user's organization tab (but not Contacts list). Average number of non-contacts in the user's organization tab is 15 users. Two contact card viewing operations per day.</li> <li>• One presence poll every time the user clicks another user to start a conversation, estimated at once per hour.</li> <li>• Six user searches per hour. Every time a search is performed, a batch poll is sent for everyone in the search result list. We assume the average size of search results is 20. If the search results stay on screen, the batch poll is refreshed every 5 minutes; we assume that there will be two such refreshes per hour.</li> <li>• When the user opens or previews an email in Outlook, a poll of the presence of users in the To: and CC: fields of the email, estimated at five emails per hour and four users per email.</li> </ul>
Presence subscriptions	<p>When one user adds another as a contact, the first user is subscribing to five categories of information about the second user. Updates of these categories of information are automatically sent to the first user.</p> <p>For each client, a single batch subscription request is sent to obtain the presence state of an average of 40 contacts, with an additional 40 dialogs to obtain presence for federated contacts.</p> <p>Presence for members of an expanded distribution group is found through persistent presence subscriptions, not polling, and is modeled as 1 expansion per user for each 2 hours.</p> <p>Short subscriptions happen when a user logs in, there is a batch subscription for all the user's contacts, and then the user soon logs off. We assume 6 short subscriptions per user per hour, where each subscription lasts 10 minutes.</p>
Presence Publication	<p>Presence state is published at an average of 4 publications per user per hour, with a maximum 6 per user per hour.</p>
Presence Document Size	<p>The average size of a complete presence document is assumed to be 4K, with a maximum of 25K.</p>

The following table describes the user model for address book use.

### Address Book Usage User Model

ADDRESS BOOK SEARCH MODE	USAGE
Address Book Web Query only (all queries performed by Address Book Web Query service)	<p>Four prefix queries per user per day.</p> <p>60 exact search queries per user per day. 40% of those are batched, with an average of 20 contacts per query. The other 60% of the queries are for a single contact.</p> <p>25 photo queries per user per day. 24 are for a single photo, the other is a batch query with an average of 20 contacts.</p> <p>One total organization search query per user per day.</p>

ADDRESS BOOK SEARCH MODE	USAGE
Mixed mode, both address book file and web queries used. This is the default mode.	Only two types of queries go to the network, the photo and total organizational search queries. 25 photo queries per user per day. 24 are for a single photo, the other is a batch query with an average of 20 contacts. One total organization search query per user per day.

The following table describes the conferencing model.

### Conferencing Model

CATEGORY	DESCRIPTION
Scheduled meetings versus "Meet now" meetings	60% scheduled, 40% unscheduled. Of the scheduled meetings, we assume that 80% are assigned conferences, which are occurrences of recurring conferences; 10% are one-time open meetings; 8% are one-time anonymous meetings, and 2% are one-time closed meetings.
Conferencing client distribution	For scheduled meetings: <ul style="list-style-type: none"> <li>• 65% of conferencing users use Skype for Business 2016.</li> <li>• 5% of conferencing users use Skype for Business Web App.</li> <li>• 30% of conferencing users use earlier clients, including Lync 2013 and Microsoft Lync 2010.</li> </ul> For unscheduled meetings: <ul style="list-style-type: none"> <li>• 70% of conferencing users use Skype for Business.</li> <li>• 30% of conferencing users use earlier clients, including Lync 2013 and Microsoft Lync 2010.</li> </ul>
Meeting concurrency	5% of users will be in conferences during working hours. Thus, in an 80,000-user pool, as many as 4,000 users might be in conferences at any one time.
Meeting audio distribution	40% mixed VoIP audio and dial-in conferencing, with a 3:1 ratio of VoIP users to dial-in users. 35% VoIP audio only. 15% dial-in conferencing audio only. 10% no audio (IM-only conferences, with an average of five messages sent per user).

CATEGORY	DESCRIPTION
Media mix for conferences	<p>75% of conferences are web conferences, which include audio plus some other collaboration modalities. For these conferences, the other collaboration methods are as follows:</p> <p><b>Note:</b> These numbers add up to more than 100% because one conference can have multiple collaboration methods.</p> <ul style="list-style-type: none"> <li>• 50% add application sharing. We assume one users sends data at a peak of 1.1 MB per second.</li> <li>• 50% add instant messaging (with an average of 2 messages per user).</li> <li>• 20% add data collaboration, including PowerPoint or whiteboard In these, an average of 2 PowerPoint files presented per conference, with an average PowerPoint file size of 10 MB (without embedded video) or 30 MB (with embedded video). Average of 20 annotations per whiteboard.</li> <li>• 20% add video. Of these users, 70% are in conferences enabled for multiview video, where each user receives 2-3 video streams.</li> <li>• 15% add shared notes.</li> </ul>
Meeting participant distribution	<p>50% internal, authenticated users.  25% remote access, authenticated users.  15% anonymous users.  10% federated users.</p>
Meeting join distribution	<p>Users are simulated as joining the meeting within the first 5 minutes.</p>

In regular Front End pools, Skype for Business Server has a maximum supported meeting size of 250 users. Each pool can host one 250-user meeting at a time. While this large meeting is occurring, the pool can also host other smaller conferences. Additionally, you can support meetings of up to 1000 users by setting up a dedicated pool to host these meetings. For details, see [Plan for large meetings in Skype for Business Server](#).

Conferences were simulated as follows:

- 85% of conferences had four participants.
- 10% of conferences had six participants.
- 5% of conferences had 11 participants.
- One large conference of 250 users.

The following table provides details about the user model for conferences involving dial-in users.

#### Dial-In Conferencing User Model

CATEGORY	DESCRIPTION
Authenticated/anonymous	<p>70% of callers join as anonymous and are prompted for a recorded name. 30% join as authenticated users.</p>
Call duration and music on hold	<p>Average call duration without music on hold: 50 seconds.  50% of call-in users hear music on hold, for an average of 5 minutes.</p>

CATEGORY	DESCRIPTION
Dual-tone multifrequency (DTMF)	15% of conferences that are dial-in only have phone leaders. 10% of mixed conferences that include dial-in users also have phone leaders. 20% of phone leaders use 2 DTMF commands per conference.
Announcement languages	Simulations use English as the announcement language.

The following table provides details about the user model for conference lobbies.

### Conference Lobby User Model

CATEGORY	DESCRIPTION
Number of users in lobby	5% of dial-in users go through the lobby, and 25% of other users go through the lobby
Admitting from lobby	In simulations, all users were admitted by the presenter before client timeout.

The following table describes the user model for other peer-to-peer sessions.

### Peer-to-Peer Sessions User Model

CATEGORY	DESCRIPTION
Application sharing	Each user participates in 5 peer-to-peer application sharing sessions per month, for an average of 0.25 sessions per day.
File transfer	Each user participates in 1 peer-to-peer file transfer session per month (as part of an IM session), for an average of 0.05 sessions per day. The average session file size transferred is 1 MB.

The following table describes the user model for policies.

### Policies User Model

CATEGORY	DESCRIPTION
Conferencing, Presence, and Archiving Policies	We assume that there is one global policy, 10 tag conferencing policies, 4 Archiving policies, and 10 tag presence policies.
Voice Policy	We assume that there is one global policy and 2 tag policies per site. 100% of sites have a site policy, and 30% of users have a per-user policy assigned. We assume one dial plan per site and two routes per site.

## Busy Hour

For peer-to-peer sessions, peak load is calculated using busy hour call attempts (BHCA). This voice industry term assumes that 50% of all calls for the day will be completed in 20% of the time. It is calculated using the following formula:

$$\text{BHCA} = (\text{total calls} * 0.5) / 1.6$$

Performance testing simulated busy hour by running VoIP and other peer-to-peer sessions at a busy hour load for at least 1.6 hours per day.

Conferencing peak load assumes that 75% of all conferences for an eight-hour day happen in 4 peak time hours. Those peak hours have 1.5 times the average conferencing load.

## Enterprise Voice to PSTN Calls

The following assumptions apply to Enterprise Voice calls:

- 60% of users are enabled for Enterprise Voice, and 60% of these users are enabled for PSTN calling.
- Each of these users enabled for PSTN calling makes 4 PSTN calls during the busy hour. Each call duration is 3 minutes.
- 65% of these PSTN voice calls use media bypass.

## Mobility

40% of registered users are assumed to be enabled for Mobility. For each user that has mobility enabled, we assume that the activity of the mobile client is additive to that of the other MPOP instances for that user, with the exception of conferencing interactions, for which the mobility client is just another client type that can be used to participate in conferences.

## Persistent Chat

We assume that 25% of registered users will be involved in Persistent chat sessions, with the following characteristics:

- An average of 1.5 chat rooms per user
- Each chat room results in 12 polling requests per hour, targeting an average of 10 users each

## Response Group and Call Park

We assume that 0.15% of registered users belong to response groups. We assume that 0.02% of registered users have parked calls at any given point of time.

# Install Skype for Business Server

8/7/2019 • 5 minutes to read

**Summary:** Learn how to prepare your environment for an installation of Skype for Business Server. Download a free trial of Skype for Business Server from the Microsoft Evaluation center at: <https://www.microsoft.com/evalcenter/evaluate-skype-for-business-server>.

This article walks you through an example installation of Skype for Business Server. This article does not attempt to cover all of the procedures you need to perform a full Skype for Business Server installation. The goal is to provide example procedures in a narrowly defined topology that includes basic meet-and-share functionality.

## Overview of the install process for Skype for Business Server

An installation of Skype for Business Server includes many different procedures. The procedures you need to get Skype for Business Server running in your environment depend on the specifics of your environment. For example, if you are using Windows Server for DNS, you will benefit from the example procedure for adding a DNS entry. If you use another system for DNS, you need to follow procedures for your particular DNS system. This is true for many of the procedures in this section.

Skype for Business Server is available in Standard Edition and Enterprise Edition. The main difference is that Standard Edition does not support the high availability features that are included with Enterprise Edition.

Skype for Business Server is an advanced product, and the exact installation process depends a great deal on your specific circumstances. This section walks you through the general steps to install the product. However, each procedure might be different depending on your environment and planning decisions. For example, for small organizations a single server, running Skype for Business Server Standard Edition might be appropriate, whereas a large multinational organization might have 50 servers at locations around the world dedicated to the product.

### NOTE

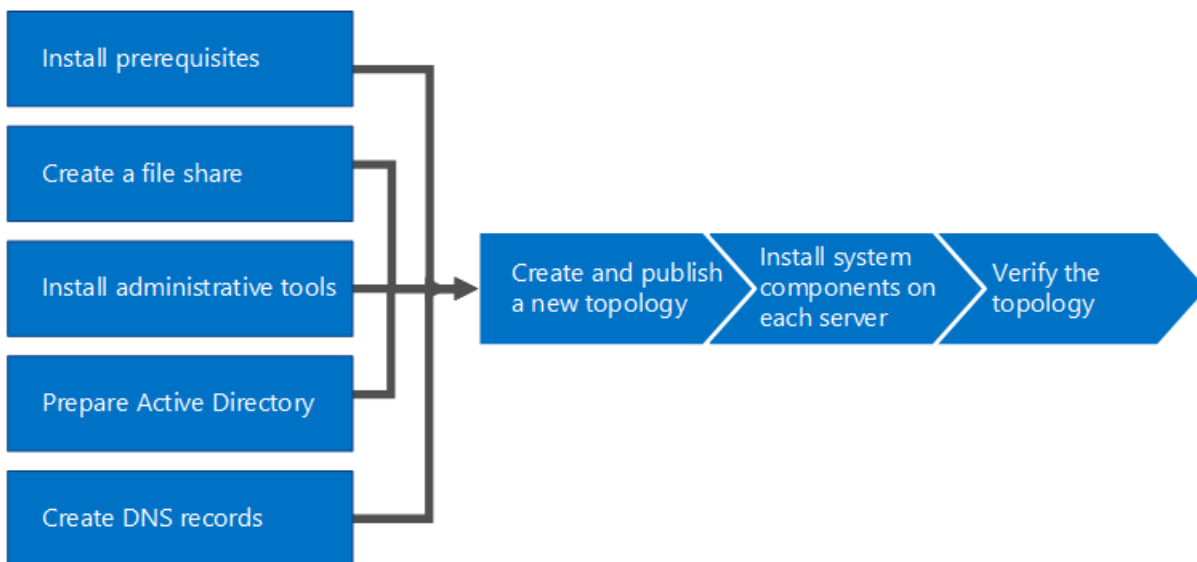
To learn about the latest Cumulative Updates, see [Updates for Skype for Business Server](#). After installing the CU1 patch an administrator needs to execute the `Update-CsAdminRole` cmdlet. This cmdlet is required to access the new GCP cmdlets over Remote PowerShell.

### IMPORTANT

The procedures in this section serve as an example using a narrowly defined set of requirements and assume specific decisions have already been made. The actual procedures you need to install Skype for Business Server will likely be very different. Use the procedures in this section as an example only and not as a step-by-step guide for installing Skype for Business Server in every environment.

Getting Skype for Business Server up and running for the first time involves eight primary steps. You should understand that the example procedures in this section are not the only procedures required for installing Skype for Business Server. The following eight steps are simply examples to help you better understand the overall process and get a basic working environment up and running. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. The eight steps are:





- **Install prerequisites for Skype for Business Server** : Install prerequisites on all servers that make up the Skype for Business Server topology. Note that prerequisites are not the same for all roles. For example, servers that provide the front-end role have a set of prerequisites, and servers that provide a director role have a different set of prerequisites. See prerequisite planning documentation for more details.
- **Create a file share in Skype for Business Server** : Create a file share that will be used by servers throughout the Skype for Business Server topology.
- **Install administrative tools in Skype for Business Server** : The administrative tools include Topology Builder and Control Panel. You must install the administrative tools on at least one server in the topology or a 64-bit management workstation running a Windows OS version that is supported for Skype for Business Server.
- **Prepare Active Directory for Skype for Business Server** : Skype for Business Server works closely with Active Directory. You must prepare the Active Directory domain to work with Skype for Business Server. You can do this through the Deployment Wizard, and it is only done once for the domain. This is because the process creates groups and modifies the domain, and you need to do that only once.
- **Create DNS records for Skype for Business Server** : In order for Skype for Business Server to work properly, a number of DNS settings must be in place. This is so that clients know how to access the services and the servers know about each other. These settings only need to be completed once per deployment because once you assign a DNS entry, it is available throughout the domain.
- **Create and publish new topology in Skype for Business Server** : Before you can install the Skype for Business Server system on each of the servers in the topology, you must create a topology and publish it. When you publish a topology, you are loading the topology information into the Central Management Store database. If this is an Enterprise Edition pool, you are creating the Central Management Store database the first time you publish a new topology. If this is Standard Edition, you need to run the Prepare First Standard Edition Server process from the Deployment Wizard before you publish a topology. This prepares for Standard Edition by installing a SQL Server Express Edition instance and creating the Central Management Store.
- **Install Skype for Business Server on servers in the topology** : Once the topology is loaded into the Central Management Store and Active Directory knows which servers will perform which roles, you need to install the Skype for Business Server system on each of the servers in the topology.
- **Verify the topology in Skype for Business Server** : After you have the topology published and the Skype for Business Server system components installed on each of the servers in the topology, you are ready to verify that the topology is working as expected. This includes verifying that the configuration has propagated out to all of the Active Directory servers so that the entire domain knows that Skype for Business is available in

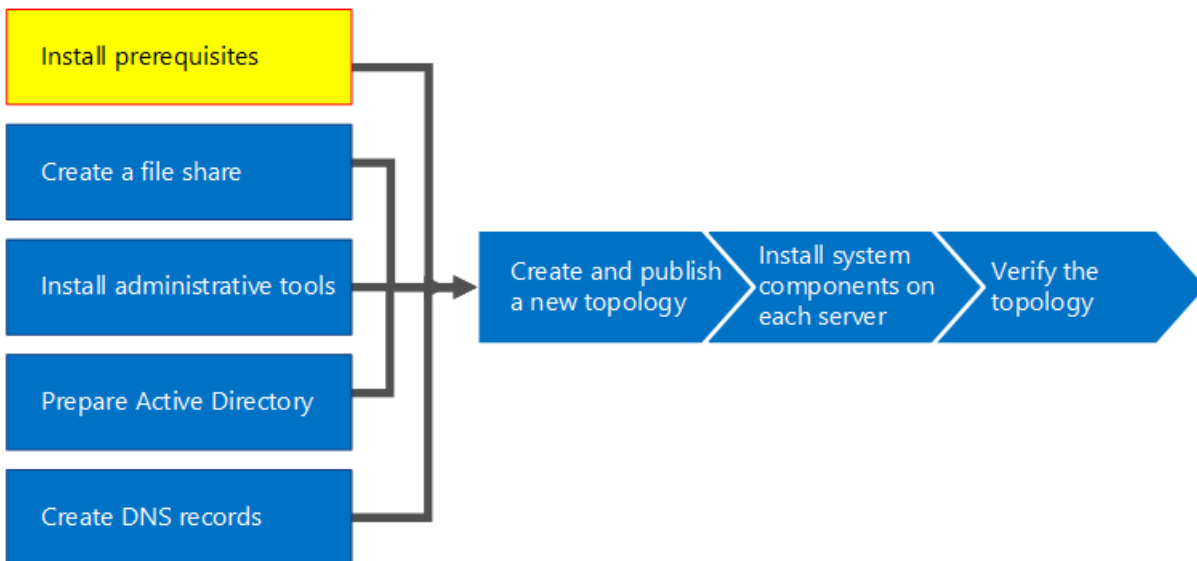
the domain.

# Install prerequisites for Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn about the servers and server roles you must configure before you install Skype for Business Server. Download a free trial of Skype for Business Server from the [Microsoft Evaluation center](#).

Installing prerequisites consists of setting up Windows Server by installing the required roles and features on each of the servers in the topology. The requirements are based on the role the server will fulfill in the topology. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. Installing prerequisites is step 1 of 8.



## Setup Windows Server

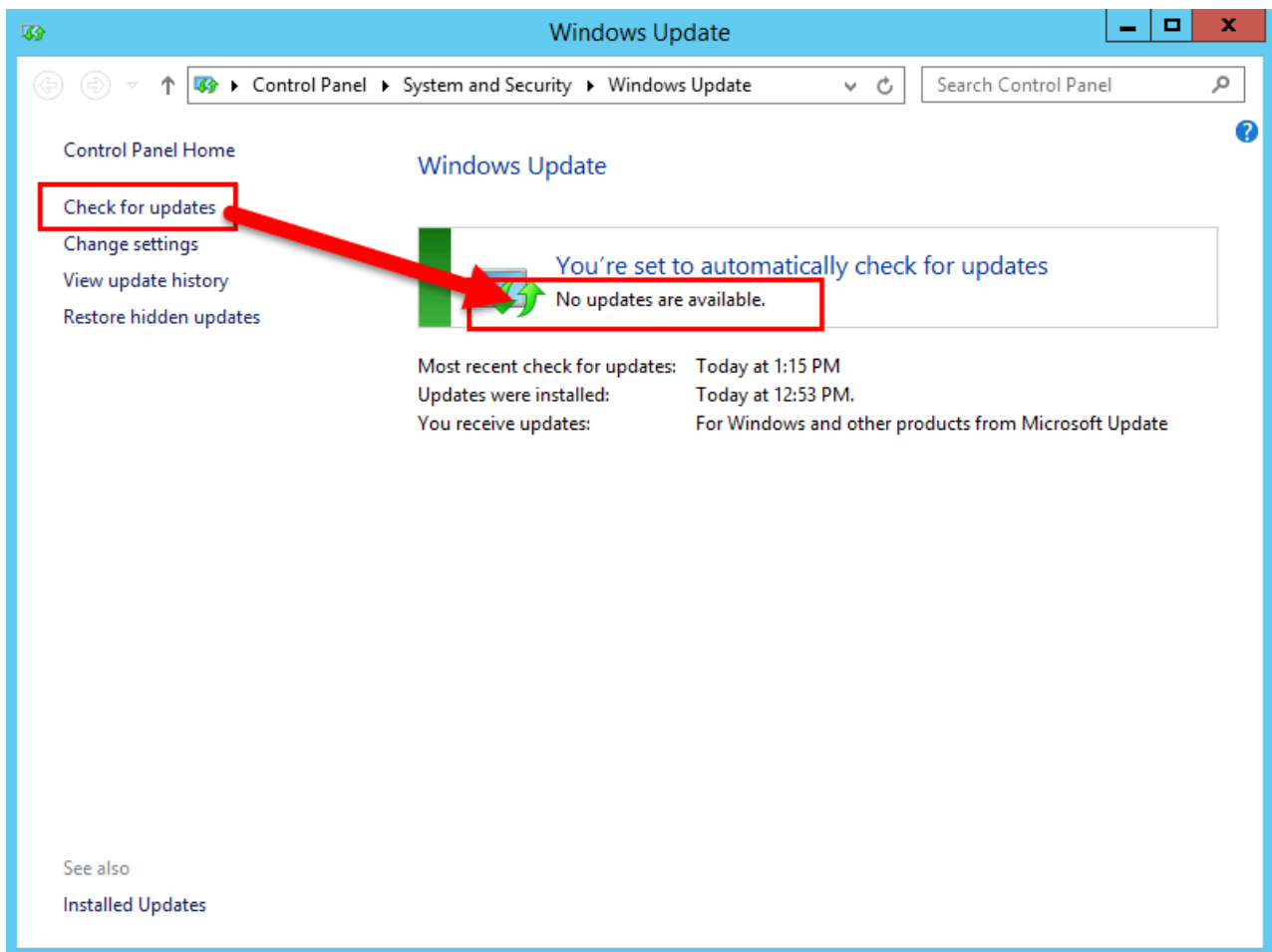
Skype for Business Server requires the Windows Server operating system and a number of prerequisites before it can be installed. For details on planning for prerequisites, see [Server requirements for Skype for Business Server](#).

### TIP

This procedure uses Windows Server 2012 R2. If you are using a different version of Windows Server, the procedure might be slightly different.

### IMPORTANT

Before you begin, make sure that Windows Server is up-to-date by using Windows Update.



Watch the video steps for **install prerequisites**:

### Install required roles and features for front-end servers

You can install the required roles and features using Server Manager.

1. Install the prerequisite software features listed in [Server requirements for Skype for Business Server](#). The required software must be on the server that will run Skype for Business Server.

#### Caution

Windows Server 2012 R2 does not install all of the source files for the required features by default. If the server is not connected to the Internet, you will need to insert the Windows Server 2012 R2 media and select **Specify an alternate source path** in order to install the required features. The source files are located in the sources\sxs directory. For example, if the Windows Server 2012 R2 media is in drive D, you would set the path to `d:\sources\sxs`. It is important that you have the latest updates from Windows Update. If you are not connected to the Internet, you will need to manually install all relevant updates as well as any prerequisites to the required updates.

2. When the dialog box indicates that the installation has completed, you will need to reboot the server to complete the process.
3. Run **Windows Update** again to check if there are any updates to the roles and services that were installed.
4. If you will be using Skype for Business Server Control Panel on this server then you must also install Silverlight. To install Silverlight, see [Microsoft Silverlight](#).

**IMPORTANT**

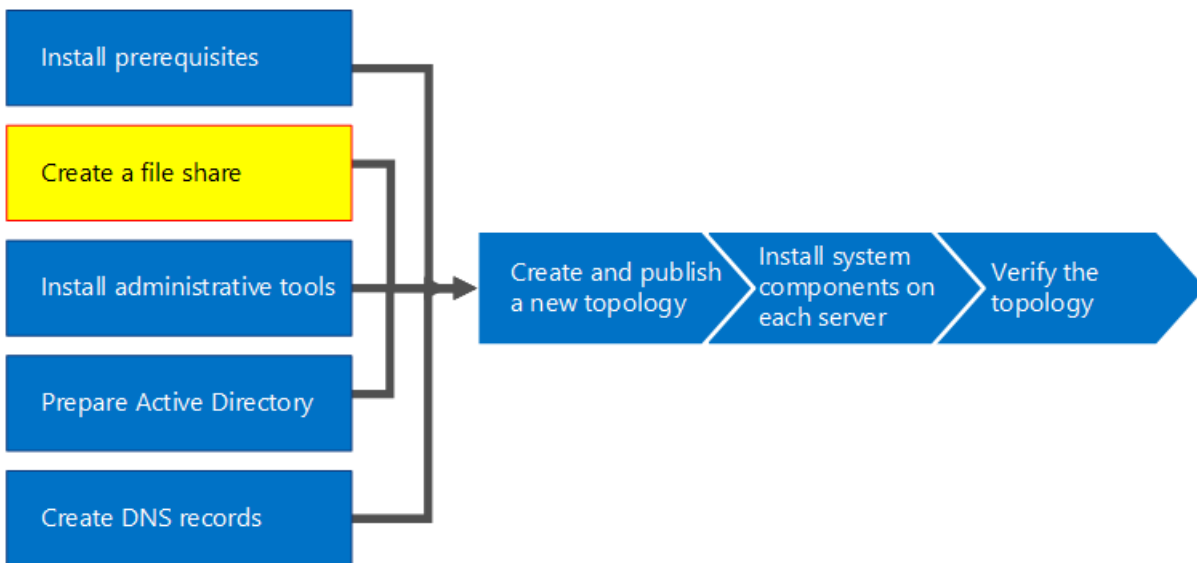
The prerequisites for servers performing roles other than front-end server, such as the role of Director, Persistent Chat, or Edge, have their own prerequisites. For details on the exact prerequisites required by each server type, see [Server requirements for Skype for Business Server](#).

# Create a file share in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to create a Windows Server file share as part of the installation of Skype for Business Server. Download a free trial of Skype for Business Server from the Microsoft Evaluation center at: <https://www.microsoft.com/evalcenter/evaluate-skype-for-business-server>.

Skype for Business Server requires a file share so that computers throughout the topology can exchange files. Creating a file share is step 2 of 8 in the installation process for Skype for Business Server. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5 as outlined in the diagram. For planning details about file share, see [Environmental requirements for Skype for Business Server](#) or [Server requirements for Skype for Business Server 2019](#).



## Create a basic file share

This section walks you through creating a basic Windows Server file share. A basic Windows Server file share is supported with Skype for Business Server. However, it does not explicitly provide high availability. For a high availability environment, a Distributed File System (DFS) file share is recommended. For more information about a high availability file share and DFS, see [Plan for high availability and disaster recovery in Skype for Business Server](#).

### NOTE

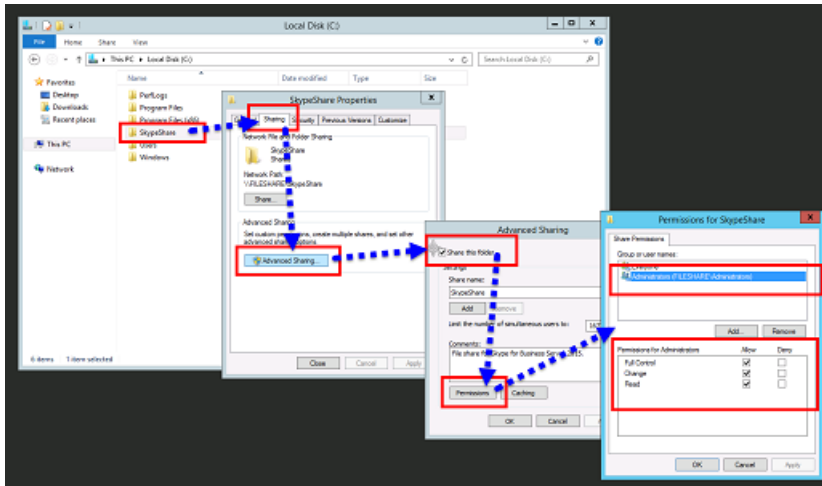
Windows Server 2012 R2 has made major leaps in providing Storage Area Network (SAN)-like file share solutions using the Windows Server platform. When compared to a traditional SAN-based appliance, a Windows Server 2012 R2 storage solution can cut costs in half with very minimal impact to performance. For more information about file share options in Windows Server 2012 R2, see the downloadable white paper [Windows Server 2012 R2 Storage](#).

Watch the video steps for **create a file share**:

### Create a basic file share

1. Log on to the computer that will host the file share.

2. Right-click the folder you plan to share, and select **Properties**.
3. Select the **Sharing** tab, and click **Advanced Sharing**.
4. Click **Share this folder**.
5. Click **Permissions**.
6. Add the local **Administrators** group of the server hosting the file share, grant **Allow: Full Control, Change, and Read** rights, and then click **OK**.
7. Click **OK** again and take note of the network path.
8. Click **Done** to close the wizard.



**NOTE**

If the file store is hosted on a DFS share, the following warning will be received:

Warning: Unable to access share permissions for "\\<share>".

This is expected if you are not an administrator on the file server, or if this is a Distributed File System (DFS) share. If the share permissions have already been configured, this warning can be ignored. If it is a new share, refer to the documentation for details on manually configuring share permissions.

Due to the inability to access the share permissions on a DFS share, Skype for Business Server will not be able to explicitly set groups on the file share. To ensure Skype for Business Server components can access the file share with the appropriate permissions, ensure the following RTC groups are added with Change level share permissions in addition to the local Administrators with Full Control share permissions.

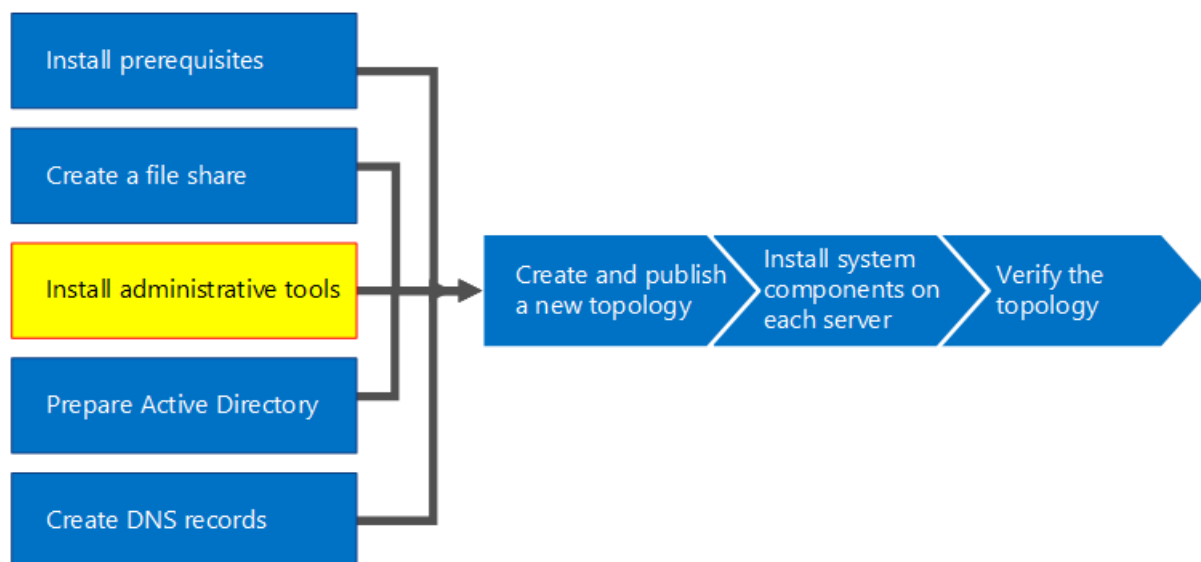
RTCHSUniversalServices RTCCComponentUniversalServices RTCUniversalServerAdmins

# Install administrative tools in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to install the administrative tools required for an installation of Skype for Business Server. Download a free trial of Skype for Business Server from the Microsoft Evaluation center at: <https://www.microsoft.com/evalcenter/evaluate-skype-for-business-server>.

The administrative tools include Topology Builder and the Control Panel. The administrative tools must be installed on at least one server in the topology or a 64-bit management workstation running a Windows OS version that is supported for Skype for Business Server. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. Installing the administrative tools is step 3 of 8.



## Install Skype for Business Server administrative tools

The installation media for Skype for Business Server provides a flexible experience. When you first run Setup.exe, the only tools installed are the Skype for Business Server Deployment Wizard and the Skype for Business Server Management Shell. By using these two tools, known as Core Components, you can continue with the installation process, but they do not provide primary functionality for the overall Skype for Business Server environment. The Deployment Wizard launches automatically after you install the Core Components. The section of the Deployment Wizard titled **Install Administrative Tools** installs Skype for Business Server Topology Builder and Skype for Business Server Control Panel.

### IMPORTANT

Every Skype for Business Server environment must have at least one server with the administrative tools installed.

Watch the video steps for **Install administrative tools**:

### Install Skype for Business Server administrative tools from the Deployment Wizard

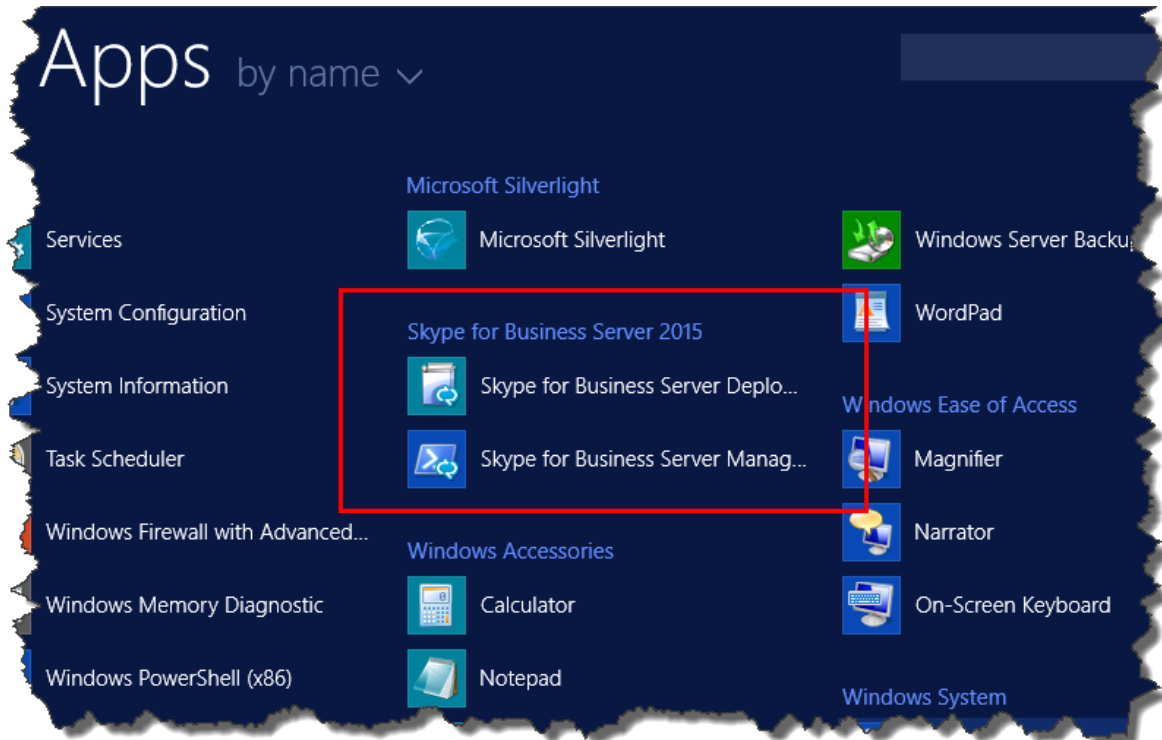
1. Insert the Skype for Business Server installation media. If the setup does not automatically begin, double-



click **Setup**.

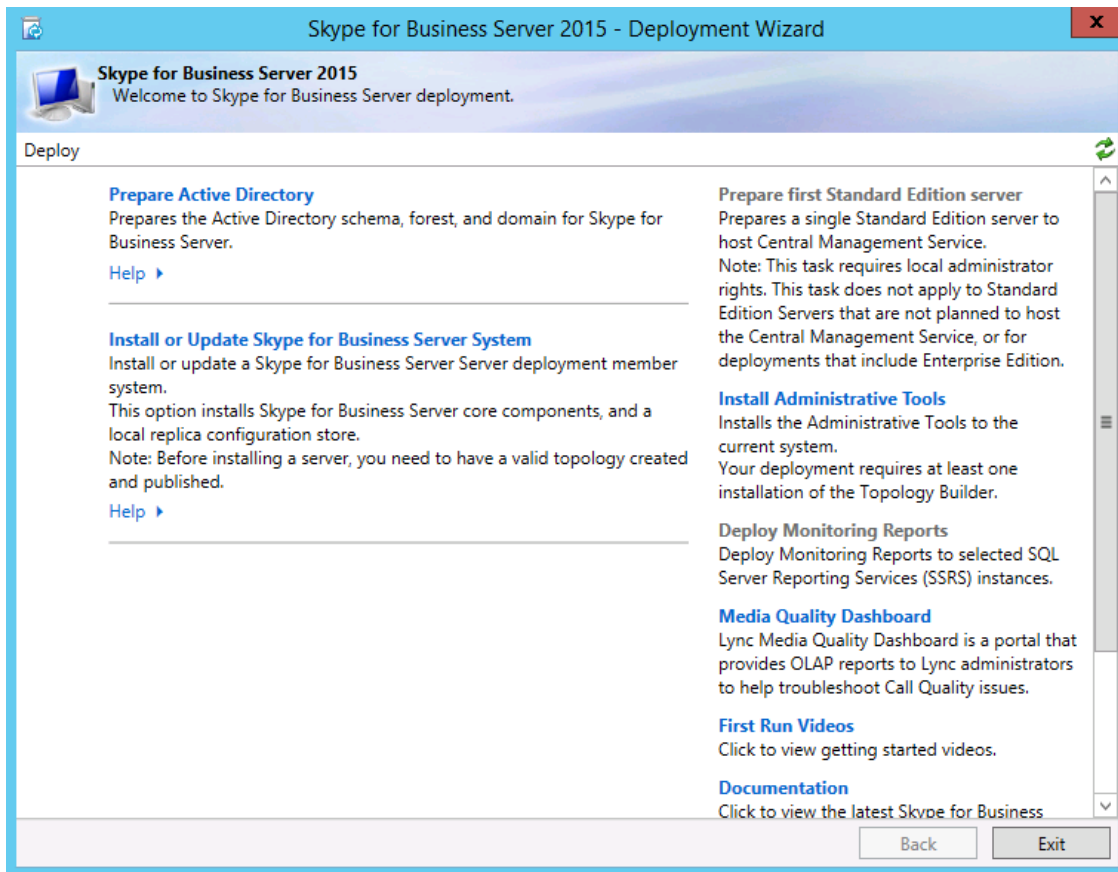
2. The installation media requires Microsoft Visual C++ to run. A dialog box will pop up asking if you want to install it. Click **Yes**.
3. By using Smart Setup, a new feature in Skype for Business Server, you can connect to the Internet to check for updates during the installation process. This provides a better experience by making sure you have the most recent updates to the product at installation. Click **Install** to begin the installation.
4. Carefully review the License Agreement, and if you agree, select **I accept the terms in the license agreement**, and click **OK**.
5. The Skype for Business Server Core Components will be installed on the server.

The Core Components consist of the following, as shown in the figure.

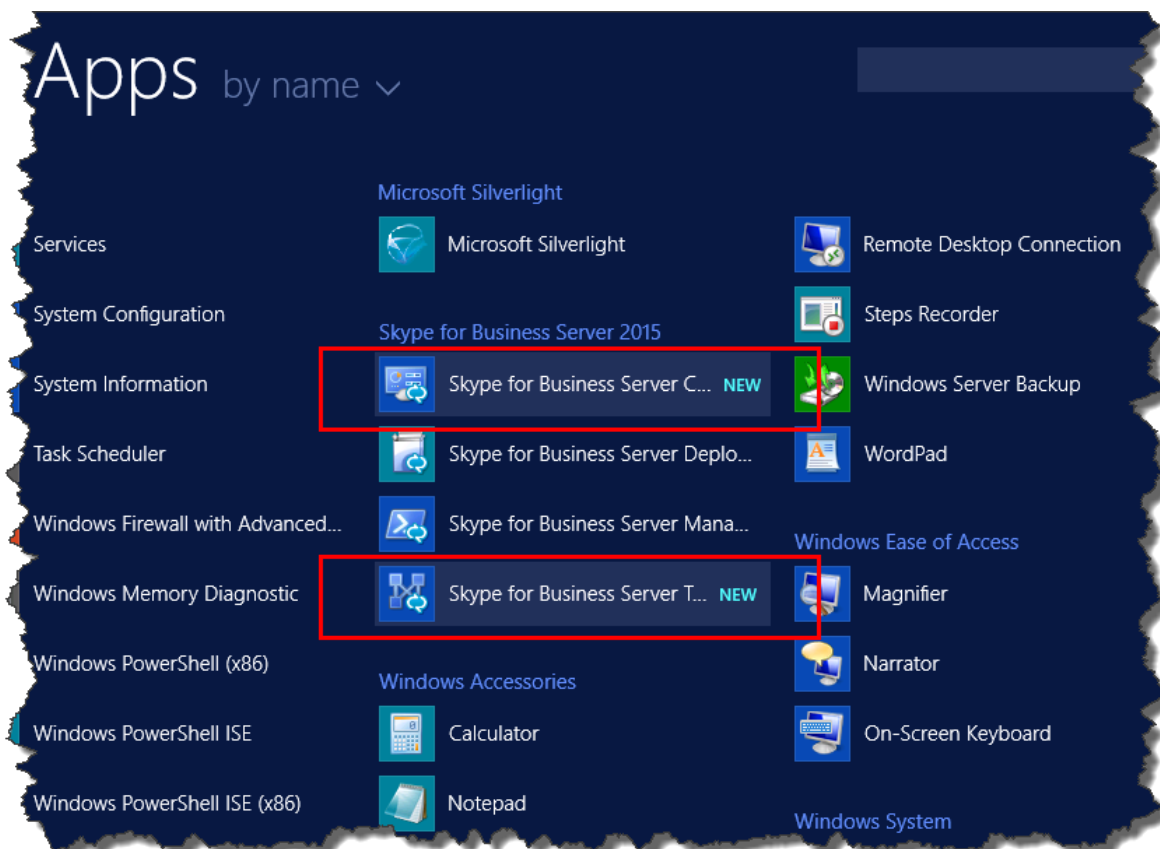


- **Skype for Business Server Deployment Wizard** A deployment program that provides a launch pad for installing the various components of Skype for Business Server.
- **Skype for Business Server Management Shell** A preconfigured PowerShell program that allows for administration of Skype for Business Server.

Once the installation of the Core Components is complete, the Skype for Business Server Deployment Wizard will automatically launch, as shown in the figure.



6. In addition to the Core Components, you will also need to install Skype for Business Server Topology Builder and Skype for Business Server Control Panel on at least one server in the environment. Click **Install Administrative Tools** on the Deployment Wizard.
7. Click **Next** to begin the installation.
8. Once the installation has completed, click **Finish**. The administrative tools are now added to the server, as shown in the figure.



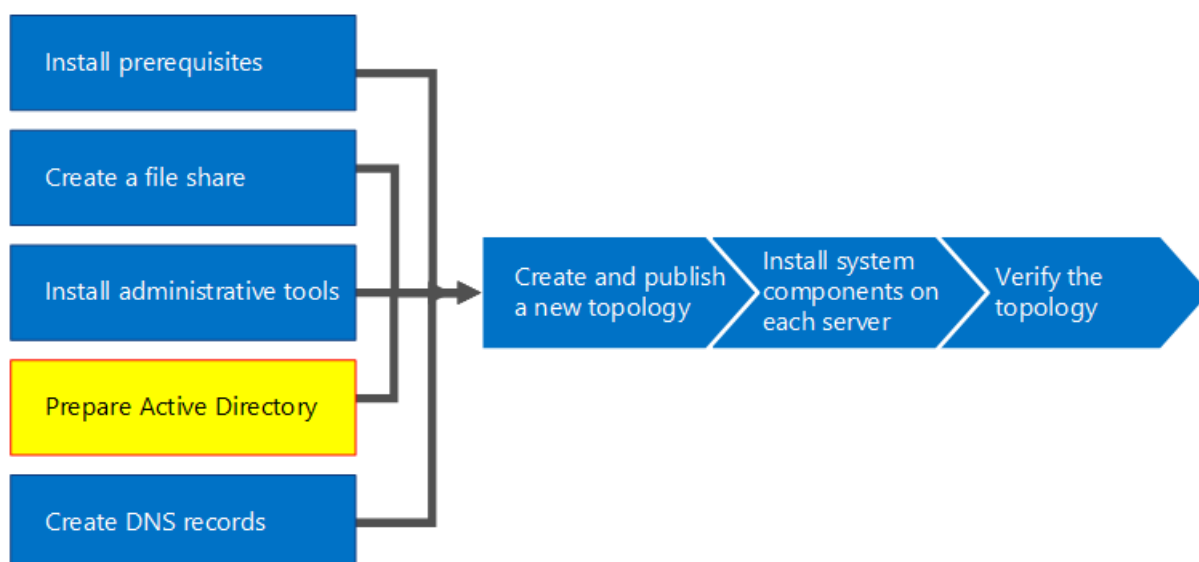
- **Skype for Business Server Topology Builder** A program used to build, deploy, and manage topologies.
- **Skype for Business Server Control Panel** A program used to administer the installation.

# Prepare Active Directory for Skype for Business Server

8/7/2019 • 7 minutes to read

**Summary:** Learn how to prepare your Active Directory domain for an installation of Skype for Business Server. Download a free trial of Skype for Business Server from the [Microsoft Evaluation Center](#).

Skype for Business Server works closely with Active Directory. You must prepare the Active Directory domain to work with Skype for Business Server. This process is accomplished in the Deployment Wizard and is only done once for the domain. This is because the process creates groups and modifies the domain, and you need to do that only once. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. Preparing Active Directory is step 4 of 8. For more information about planning for Active Directory, see [Environmental requirements for Skype for Business Server](#) or [Server requirements for Skype for Business Server 2019](#).



## Prepare Active Directory

Skype for Business Server is tightly integrated with Active Directory Domain Services (AD DS). Before Skype for Business Server can be installed for the first time, Active Directory must be prepared. The section of the Deployment Wizard titled **Prepare Active Directory** prepares the Active Directory environment for use with Skype for Business Server.

### NOTE

Skype for Business Server uses (AD DS) to track and communicate with all of the servers in a topology. Every server must be joined to the domain so that Skype for Business Server can work properly.

### IMPORTANT

The Prepare Active Directory procedure should be run only once for each domain in the deployment.

Watch the video steps for **Prepare Active Directory**:

## Prepare Active Directory from the Deployment Wizard

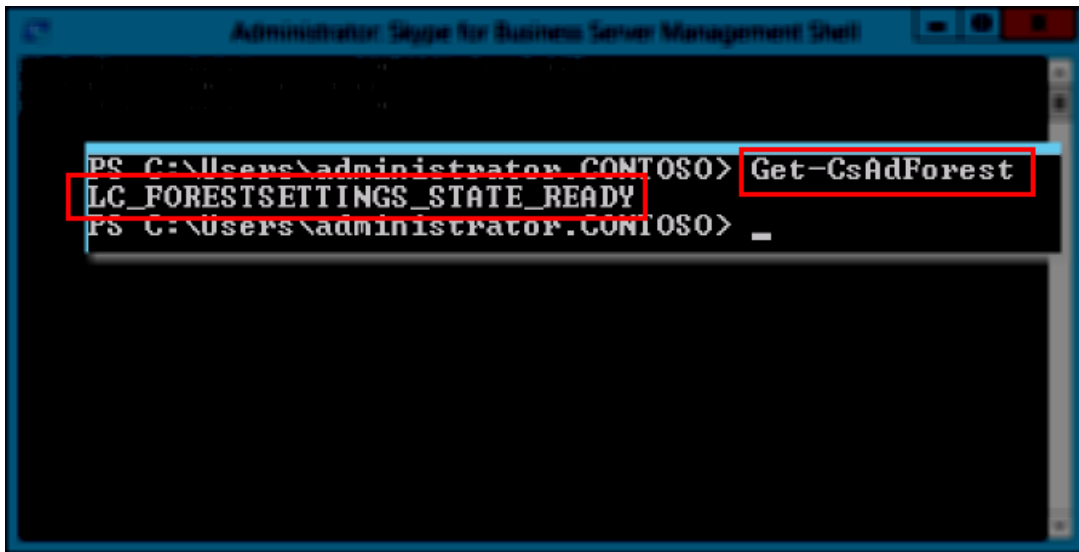
1. Log on as a user with Schema Admins credentials for the Active Directory domain.
2. Open Skype for Business Server Deployment Wizard.

### TIP

If you want to review the log files that are created by the Skype for Business Server Deployment Wizard, you can find them on the computer where the Deployment Wizard was run, in the Users directory of the AD DS user who ran the step. For example, if the user logged on as the domain administrator in the domain, contoso.local, the log files are located in: C:\Users\Administrator.Contoso\AppData\Local\Temp.

3. Click the **Prepare Active Directory** link.
4. **Step 1: Prepare schema**
  - a. Review the prerequisites information for Step 1 which can be accessed by clicking the drop-down under the Step 1 title.
  - b. Click **Run** in Step 1 to launch the Prepare Schema wizard.
  - c. Take note that the procedure should be run only once for each deployment, and then click **Next**.
  - d. Once the schema has been prepared, you can view the log by clicking **View Log**.
  - e. Click **Finish** to close the Prepare Schema wizard, and return to the Prepare Active Directory steps.
5. **Step 2: Verify replication of schema partition**
  - a. Log on to the domain controller for the domain.
  - b. Open **ADSI Edit** from the **Tools** drop-down menu in **Server Manager**.
  - c. On the **Action** menu, click **Connect to**.
  - d. In the **Connection Settings** dialog box under **Select a well known Naming Context**, select **Schema**, and then click **OK**.
  - e. Under the schema container, search for **CN=ms-RTC-SIP-SchemaVersion**. If this object exists, and the value of the **rangeUpper** attribute is 1150 and the value of the **rangeLower** attribute is 3, the schema was successfully updated and replicated. If this object does not exist or the values of the **rangeUpper** and **rangeLower** attributes are not as specified, the schema was not modified or has not replicated.
6. **Step 3: Prepare current forest**
  - a. Review the prerequisites information for Step 3 which can be accessed by clicking the drop-down under the Step 3 title.
  - b. Click **Run** in Step 3 to launch the Prepare Current Forest wizard.
  - c. Take note that the procedure should be only run once per deployment, and then click **Next**.
  - d. Specify the domain where the universal groups will be created. If the server is part of the domain, you can choose **Local domain**, and click **Next**.
  - e. Once the forest has been prepared, you can view the log by clicking **View Log**.
  - f. Click **Finish** to close the Prepare Current Forest wizard, and return to the Prepare Active Directory steps.

- g. Click **Skype for Business Server Management Shell** from the **Apps** page to launch PowerShell.
- h. Type the command `Get-CsAdForest`, and press **Enter**.
- i. If the result is `LC_FORESTSETTINGS_STATE_READY`, the forest has successfully been prepared, as shown in the figure.



#### 7. Step 4: Verify replication of the global catalog

- a. On a domain controller (preferably in a remote site from the other domain controllers), in the forest where the Forest Preparation was run, open **Active Directory Users and Computers**.
- b. In **Active Directory Users and Computers**, expand the domain name of your forest or a child domain.
- c. Click the **Users** container on the left side pane, and look for the Universal group **CsAdministrator** in the right side pane. If CsAdministrator (among other new Universal groups that begin with Cs) is present, Active Directory replication has been successful.
- d. If the groups are not yet present, you can force the replication, or wait 15 minutes and refresh the right side pane. When the groups are present, replication is complete.

#### 8. Step 5: Prepare the current domain

- a. Review the prerequisites information for Step 5.
- b. Click **Run** in Step 5 to launch the Prepare Current Domain wizard.
- c. Take note that the procedure should only be run once for each domain in the deployment, and then click **Next**.
- d. Once the domain has been prepared, you can view the log by clicking **View Log**.
- e. Click **Finish** to close the Prepare Current Domain wizard, and return to the Prepare Active Directory steps.

These steps must be completed in every domain where Skype for Business Server objects are found, otherwise services might not start. This includes any type of Active Directory object, such as users, contact objects, administrative groups, or any other type of object. You can use `Set-CsUserReplicatorConfiguration -ADDomainNamingContextList` to add only the domains with Skype for Business Server objects, if needed.

#### 9. Step 6: Verify replication in the domain

- a. Click the **Skype for Business Server Management Shell** from the **Apps** page to launch PowerShell.
- b. Use the command `Get-CsAdDomain` to verify replication within the domain.

```
Get-CsAdDomain [-Domain <Fqdn>] [-DomainController <Fqdn>] [-GlobalCatalog <Fqdn>] [-GlobalSettingsDomainController <Fqdn>]
```

#### NOTE

If you do not specify the Domain parameter, the value is set to the local domain.

Example of running the command for the contoso.local domain:

```
Get-CsAdDomain -Domain contoso.local -GlobalSettingsDomainController dc.contoso.local
```

#### NOTE

By using the parameter GlobalSettingsDomainController, you can indicate where global settings are stored. If your settings are stored in the System container (which is typical with upgrade deployments that have not had the global setting migrated to the Configuration container), you define a domain controller in the root of your AD DS forest. If the global settings are in the Configuration container (which is typical with new deployments or upgrade deployments where the settings have been migrated to the Configuration container), you define any domain controller in the forest. If you do not specify this parameter, the cmdlet assumes that the settings are stored in the Configuration container and refers to any domain controller in Active Directory.

c. If the result is **LC\_DOMAINSETTINGS\_STATE\_READY**, the domain has successfully replicated.

### 10. Step 7: Add users to provide administrative access to the Skype for Business Server Control Panel

- a. Log on as a member of the Domain Admins group or the RTCUniversalServerAdmins group.
- b. Open **Active Directory Users and Computers**, expand your domain, click the **Users** container, right-click CSAdministrator, and choose **Properties**.
- c. In **CSAdministrator Properties**, click the **Members** tab.
- d. On the **Members** tab, click **Add**. In **Select Users, Contacts, Computers, Service Accounts, or Groups**, locate the **Enter the object names to select**. Type the user name(s) or group name(s) to add to the group CSAdministrators. Click **OK**.
- e. On the **Members** tab, confirm that the users or groups that you selected are present. Click **OK**.

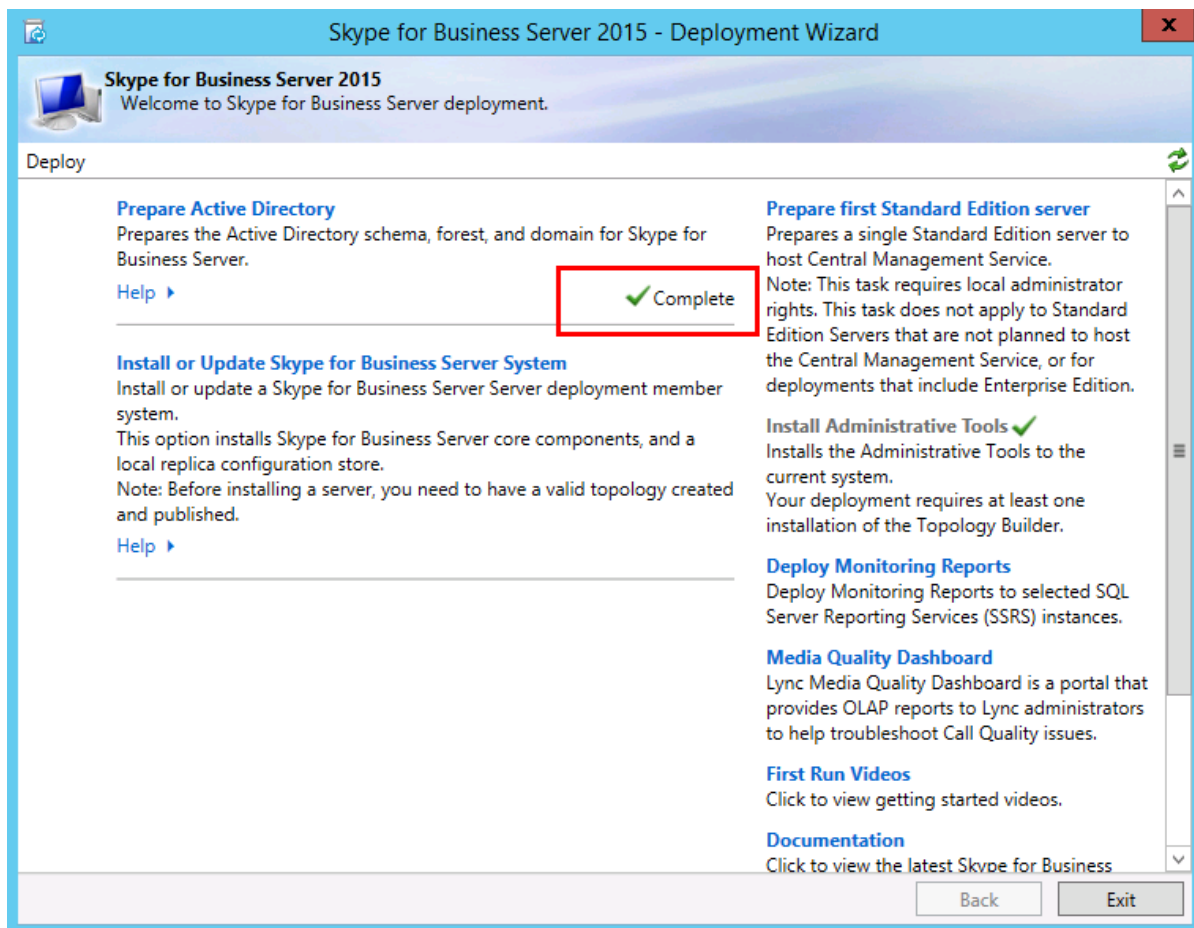
#### Caution

The Skype for Business Server Control Panel is a role-based access control tool. Membership in the CsAdministrator group gives a user who is using the Skype for Business Server Control Panel full control for all configuration functions available. There are other roles available that are designed for specific functions. For details on the roles available, see [Environmental requirements for Skype for Business Server](#) or [Server requirements for Skype for Business Server 2019](#). Note that users do not have to be enabled for Skype for Business Server in order to be made members of the management groups.

#### Caution

To help retain security and role-based access control integrity, add users to the groups that define what role the user performs in management of the Skype for Business Server deployment.

11. Log off, and then log back on to Windows so that your security token is updated with the new Skype for Business Server security group, and then reopen the Deployment Wizard.
12. Verify that you see a green checkmark next to **Prepare Active Directory** to confirm success, as shown in the figure.



## See also

[Active Directory Domain Services for Skype for Business Server 2015](#)



# Create DNS records for Skype for Business Server

8/7/2019 • 5 minutes to read

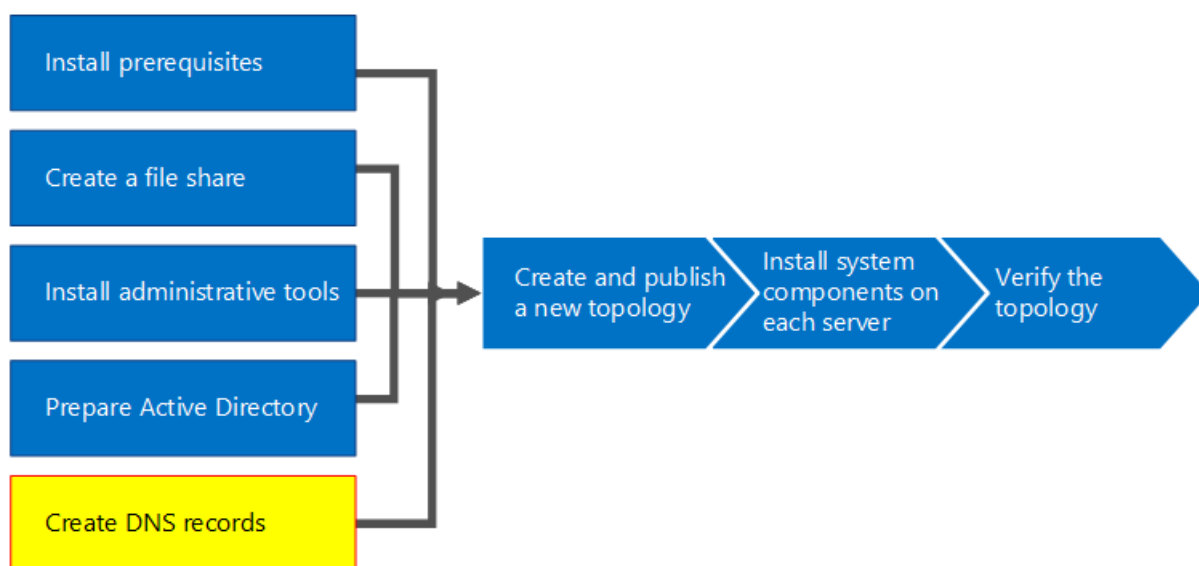
**Summary:** Learn how to configure DNS and create DNS records for an installation of Skype for Business Server. Download a free trial of Skype for Business Server from the Microsoft Evaluation center at:

<https://www.microsoft.com/evalcenter/evaluate-skype-for-business-server>.

For Skype for Business Server to work properly, a number of Domain Name System (DNS) settings must be in place. This is so that clients know how to access the services and that the servers know about each other. These settings need to be completed only once per deployment because once you assign a DNS entry, it is available throughout the domain. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. Creating DNS records comprises step 5 of 8. For more information about planning DNS, see [Environmental requirements for Skype for Business Server](#) or [Server requirements for Skype for Business Server 2019](#).

## IMPORTANT

It is important to note that this is just an example of how to create DNS records in a Windows Server DNS environment. There are many other DNS entries that are required for Skype for Business Server, and the procedure for creating DNS records depends on the system you are using to manage DNS in your organization. For a complete list of requirements for DNS, see [DNS requirements for Skype for Business Server](#).



## Configure DNS

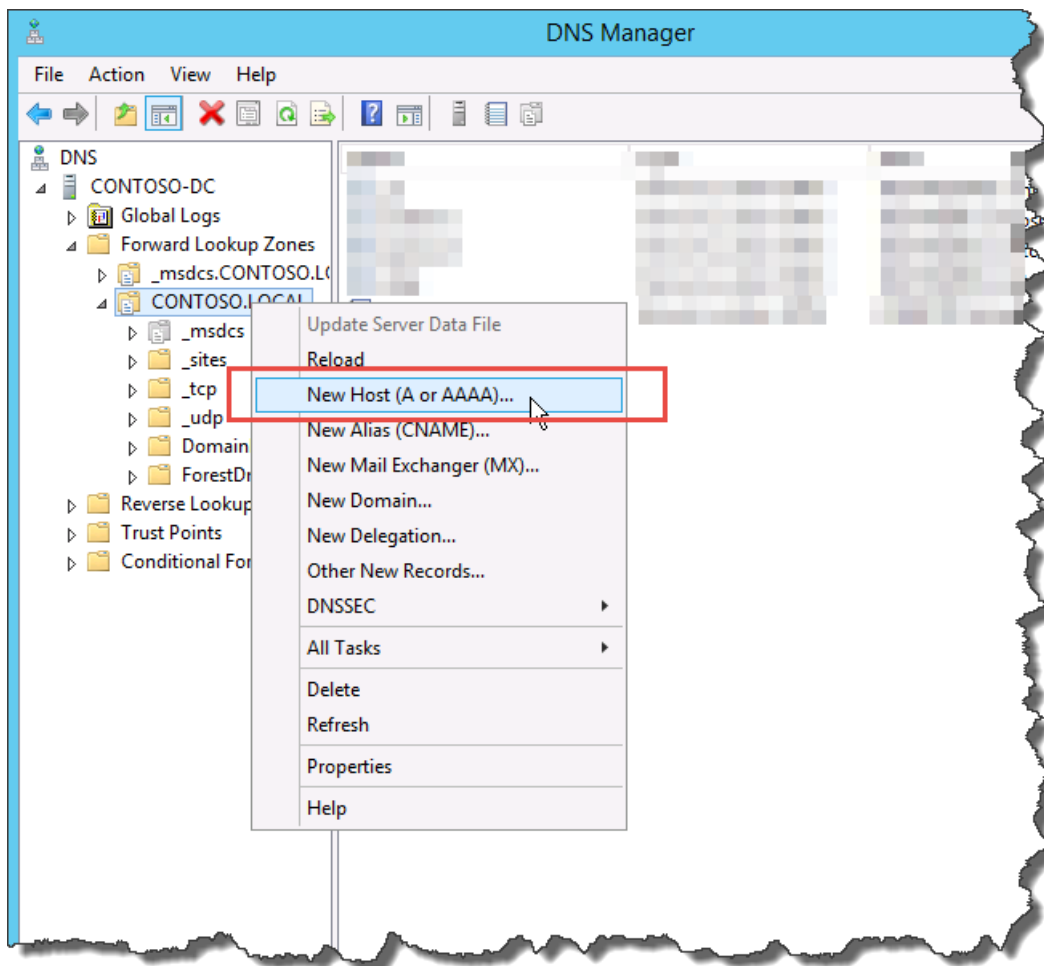
DNS records are required for Skype for Business Server to work properly and be accessible by users.

This example is using a DNS load balanced FQDN named pool.contoso.local. This pool consists of three servers running Skype for Business Server Enterprise Edition. A Standard Edition front-end server can only contain a single server. By using Standard Edition, you would only use the fully qualified domain name (FQDN) of the single Standard Edition server when referencing the front-end role instead of creating a DNS load balanced pool of servers, as this example shows. This simple example that uses only the front-end role includes the DNS entries in the following table. To plan your specific DNS requirements, see [DNS requirements for Skype for Business Server](#).

DESCRIPTION	RECORD TYPE	NAME	RESOLVES TO	LOAD BALANCING TYPE
Internal Web Services FQDN	A	webint.contoso.local	VIP for Internal Web Services	Supported software and hardware
Pool FQDN	A	pool.contoso.local	IP address of server SFB01	DNS
SFB01 FQDN	A	SFB01.contoso.local	IP address of server SFB01	DNS
Pool FQDN	A	pool.contoso.local	IP address of server SFB02	DNS
SFB02 FQDN	A	SFB02.contoso.local	IP address of server SFB02	DNS
Pool FQDN	A	pool.contoso.local	IP address of server SFB03	DNS
SFB03 FQDN	A	SFB03.contoso.local	IP address of server SFB03	DNS
Skype for Business Auto Discover	A	lyncdiscoverinternal.contoso.local	VIP for Internal Web Services	Supported software and hardware
Meeting Simple URL	A	meet.contoso.local	VIP for Internal Web Services	Supported software and hardware
Dial-in Simple URL	A	dialin.contoso.local	VIP for Internal Web Services	Supported software and hardware
Web Scheduler Simple URL	A	scheduler.contoso.local	VIP for Internal Web Services	Supported software and hardware
Administration Simple URL	A	admin.contoso.local	VIP for Internal Web Services	Supported software and hardware
Legacy Discovery	SRV	_sipinternaltls._tcp.contoso.local	Pool FQDN (port 5061)	N/A

### Create DNS records

1. Log on to the DNS server, and open **Server Manager**.
2. Click the **Tools** drop-down menu, and click **DNS**.
3. In the console tree for your SIP domain, expand **Forward Lookup Zones**, and then expand the SIP domain in which Skype for Business Server will be installed.
4. Right-click the SIP domain, and select **New Host (A or AAAA)**, as shown in the figure.



5. In the **Name** box, type the name of the host record (the domain name will be automatically appended).
6. In the **IP Address box**, type the IP address of the individual front-end server, and then select **Create associated pointer (PTR) record** or **Allow any authenticated user to update DNS records with the same owner name**, if applicable. Note that this assumes that DNS is used to load balance all traffic with the exception of web services. In this example, we have three front-end servers as shown in the table.

SERVER NAME	TYPE	DATA
SFB01	Host (A)	10.0.0.5
SFB02	Host (A)	10.0.0.6
SFB03	Host (A)	10.0.0.7

7. Next, create the DNS load balancing entries for the pool. DNS load balancing allows DNS to send requests to the individual servers in the pool while using the same DNS pool name. For more information about DNS and load balancing, see [DNS requirements for Skype for Business Server](#).

**NOTE**

Pooling multiple servers together is available only in Enterprise Edition deployments. If you are deploying a single Enterprise Server or Standard Edition server, you need to create only an A record for the single server.

For example, if you had a pool named pool.contoso.local and three front-end servers, you would create the following DNS entries:

FQDN	TYPE	DATA
pool.contoso.local	Host (A)	10.0.0.5
pool.contoso.local	Host (A)	10.0.0.6
pool.contoso.local	Host (A)	10.0.0.7

8. Continue creating A records for all servers in the planned deployment.
9. To create the service record (SRV) record for legacy discovery, right-click the SIP domain, and select **Other New Records**.
10. In **Select a resource record type**, click **Service Location (SRV)**, and then click **Create Record**.
11. Click **Service**, and then type **\_sipinternaltls**.
12. Click **Protocol**, and then type **\_tcp**.
13. Click **Port Number**, and then type **5061**.
14. Click **Host offering this service**, and then type the FQDN of the pool or Standard Edition server.

The screenshot shows a 'New Resource Record' dialog box with the following fields and values:

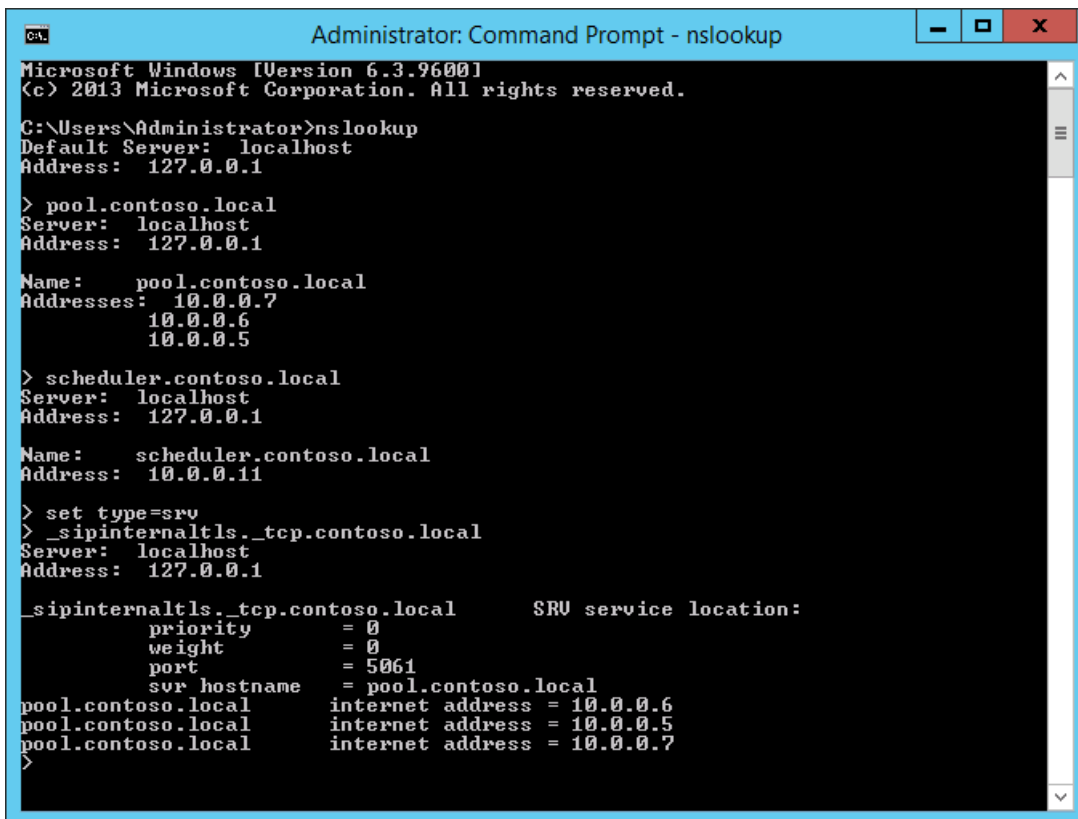
- Service Location (SRV) tab selected.
- Domain: CONTOSO.LOCAL
- Service: \_sipinternaltls
- Protocol: \_tcp
- Priority: 0
- Weight: 0
- Port number: 5061
- Host offering this service: pool.contoso.local
- Checkbox:  Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
- Buttons: OK, Cancel, Help

15. Click **OK**, and then click **Done**.

### Verify DNS records

1. Log on to a client computer in the domain with an account that is a member of the Authenticated Users group or has equivalent permissions.
2. Click **Start**, and then type **cmd**, and press Enter.
3. Type **nslookup <FQDN of the Front End pool>** or **<FQDN of the Standard Edition server or single Enterprise Edition server>**, and press Enter.
4. Continue to verify the rest of the A records for your deployment.
5. If you are supporting legacy clients and created the SRV record, verify it by typing **set type=srv** at the **nslookup** prompt, and then press Enter.

- Type **\_sipinternaltls.\_tcp.domain** (for example, **\_sipinternaltls.\_tcp.contoso.local**), and then press Enter.
- The expected output should be similar to that shown in the figure. Note that not all DNS records are shown in the sample output, but all records should be verified.



```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server: localhost
Address: 127.0.0.1

> pool.contoso.local
Server: localhost
Address: 127.0.0.1

Name: pool.contoso.local
Addresses: 10.0.0.7
           10.0.0.6
           10.0.0.5

> scheduler.contoso.local
Server: localhost
Address: 127.0.0.1

Name: scheduler.contoso.local
Address: 10.0.0.11

> set type=srv
> _sipinternaltls._tcp.contoso.local
Server: localhost
Address: 127.0.0.1

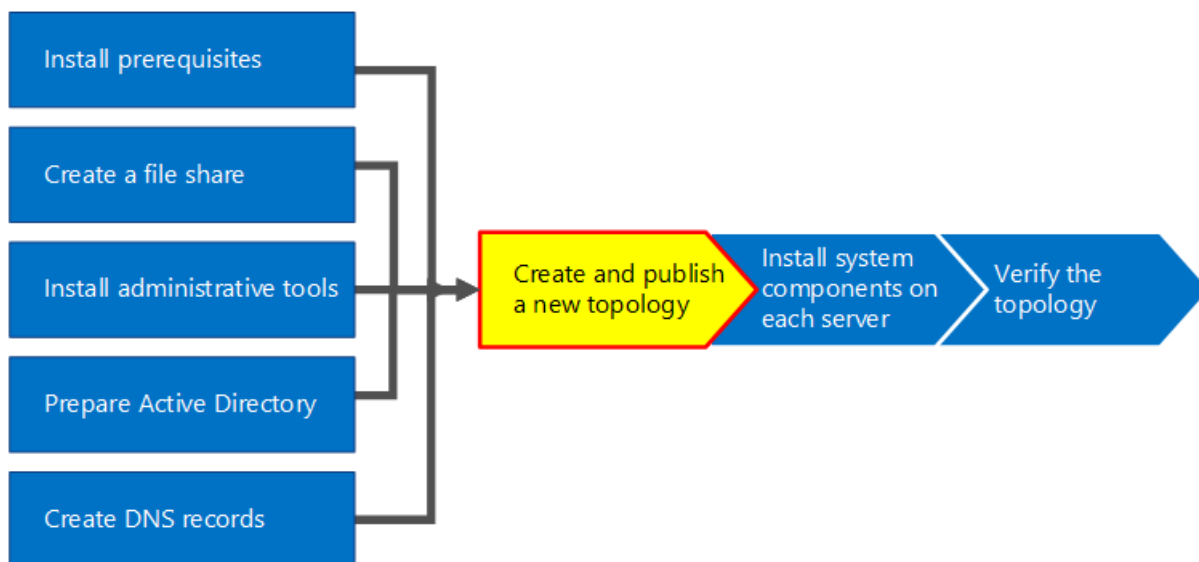
_sipinternaltls._tcp.contoso.local SRV service location:
      priority = 0
      weight   = 0
      port     = 5061
      srv hostname = pool.contoso.local
pool.contoso.local internet address = 10.0.0.6
pool.contoso.local internet address = 10.0.0.5
pool.contoso.local internet address = 10.0.0.7
>
```

# Create and publish new topology in Skype for Business Server

8/7/2019 • 16 minutes to read

**Summary:** Learn how to create, publish, and verify a new topology before you install Skype for Business Server. Download a free trial of Skype for Business Server from the Microsoft Evaluation center at: <https://www.microsoft.com/evalcenter/evaluate-skype-for-business-server>.

Before you can install the Skype for Business Server system on each of the servers in the topology, you must create a topology and publish it. When you publish a topology, you are loading the topology information into the Central Management Store database. If this is an Enterprise Edition pool, you are creating the Central Management Store database the first time you publish a new topology. If this is Standard Edition, you will need to run the Prepare First Standard Edition Server process from the Deployment Wizard before you publish a topology. This prepares for Standard Edition by installing a SQL Server Express Edition instance and creating the Central Management Store. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. How to create and publish a new topology is described in step 6 of 8.



## Create and publish new topology

You can use Skype for Business Server Topology Builder to design, define, configure, and publish topologies. This tool was installed when you installed Administrative Tools earlier in the article. There are many different choices you can make when you create a topology. In this procedure, you will create a basic topology with conferencing.

## IMPORTANT

Skype for Business Server requires SQL Server in order to operate. The primary databases are known as the Central Management Store. If you are deploying Enterprise Edition, these databases are created when you publish the topology by using the steps below. In this case, Topology Builder will ask you for the connection information to a SQL Server installation. If you are planning to deploy Standard Edition, you will need to install SQL Server Express Edition before you define and publish the new topology. To install SQL Server Express Edition, you should open the Deployment Wizard on the server that will act as the Front End, and then run Prepare First Standard Edition Server. When you click Prepare First Standard Edition Server, the Deployment Wizard automatically installs SQL Server Express Edition and creates the Central Management Store databases.

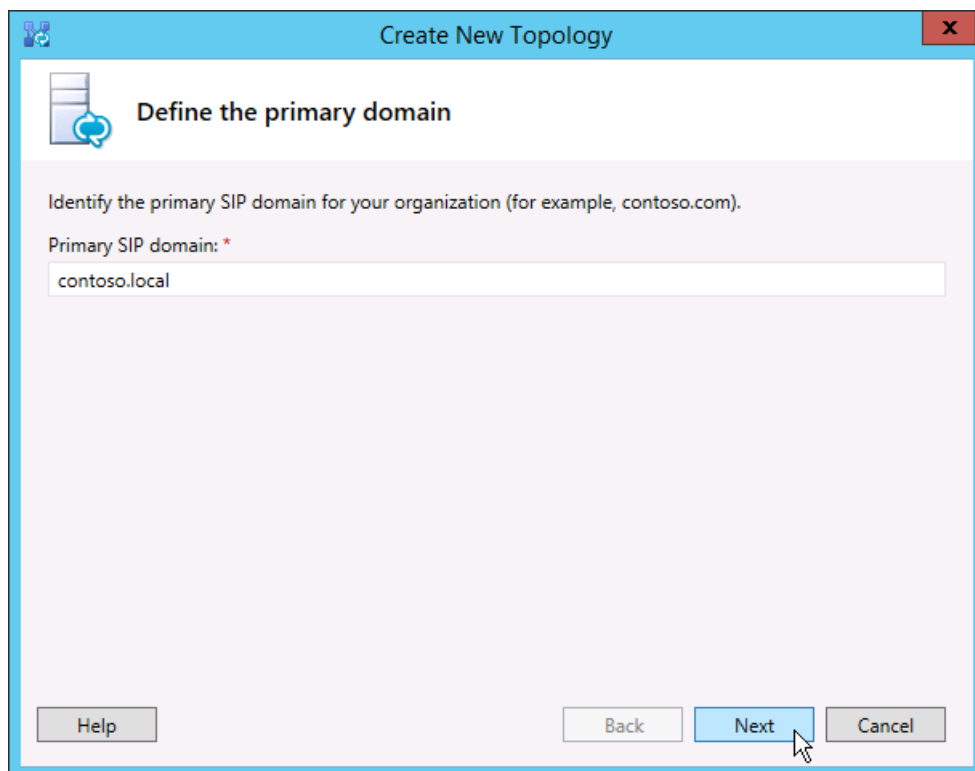
## Create a new topology

1. Log in as a standard user with access to Topology Builder.
2. Open Skype for Business Server Topology Builder.
3. Select **New Topology**, and click **OK**.
4. Select a location and file name for the topology configuration file.

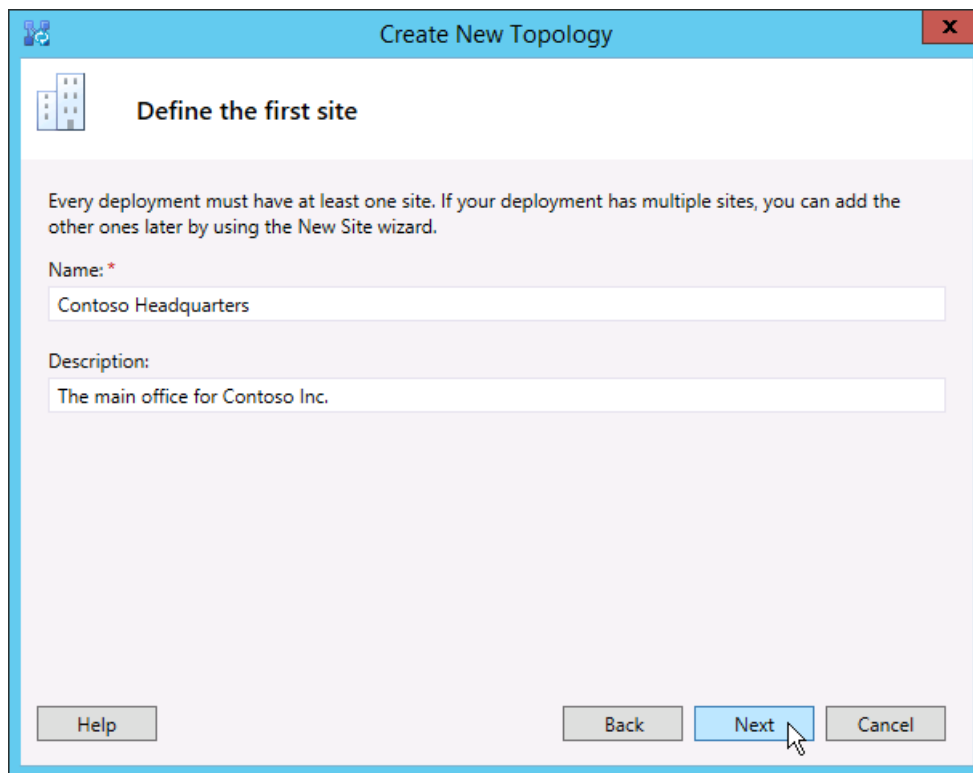
## NOTE

The topology configuration is saved as a Topology Builder XML (.tbxml) file. When you publish a topology, you are pushing the configuration information from the file to the SQL Server database. When you open Topology Builder in the future, you can download the existing configuration from SQL Server directly into Topology Builder and either publish it back to SQL Server or save it as a Topology Builder configuration file.

5. On the **Define the primary domain screen**, enter the **primary SIP domain**, and click **Next**. In this example, we are using **contoso.local**, as shown in the figure.



6. Add any additional supported SIP domains, and then click **Next**.
7. Enter a **Name** and **Description** for the first site (location), and then click **Next**, as shown in the figure.



8. Enter the **City, State/Province,** and **Country/Region Code** for the site, and then click **Next**.
9. Click **Finish** to complete the process of defining a new topology. The New Front End Wizard launches automatically.

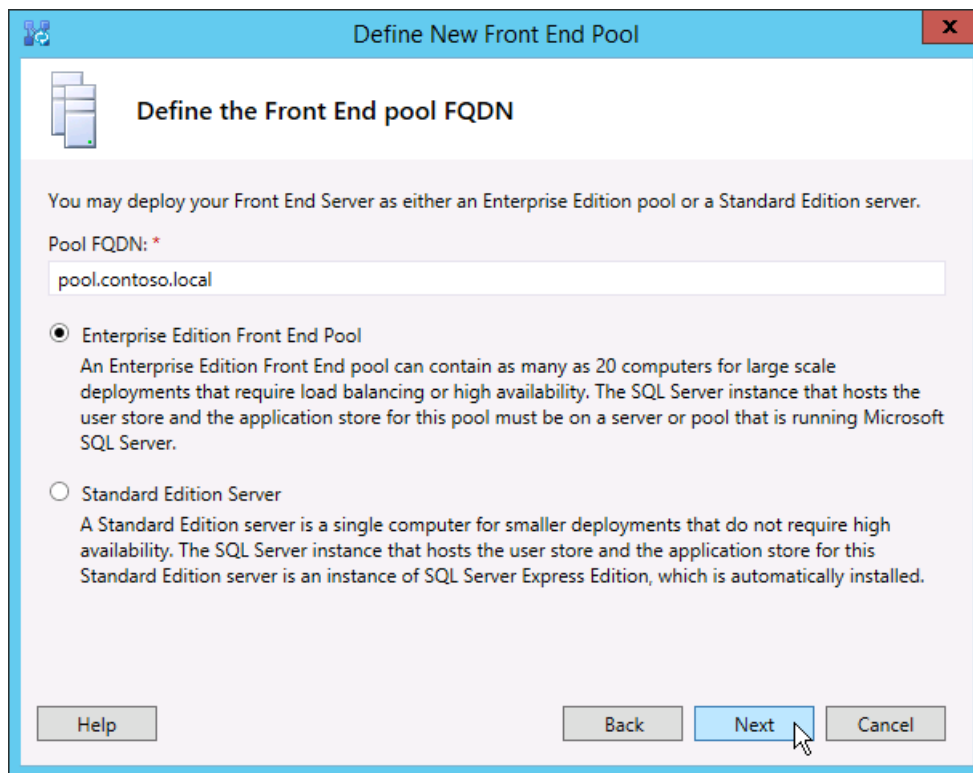
#### **Define a Front End pool or Standard Edition server**

1. Review the wizard prerequisites, and then click **Next**.
2. Enter the fully qualified domain name (FQDN) of the pool, and select either **Enterprise Edition Front End Pool** or **Standard Edition Server**, and then click **Next**, as shown in the figure.

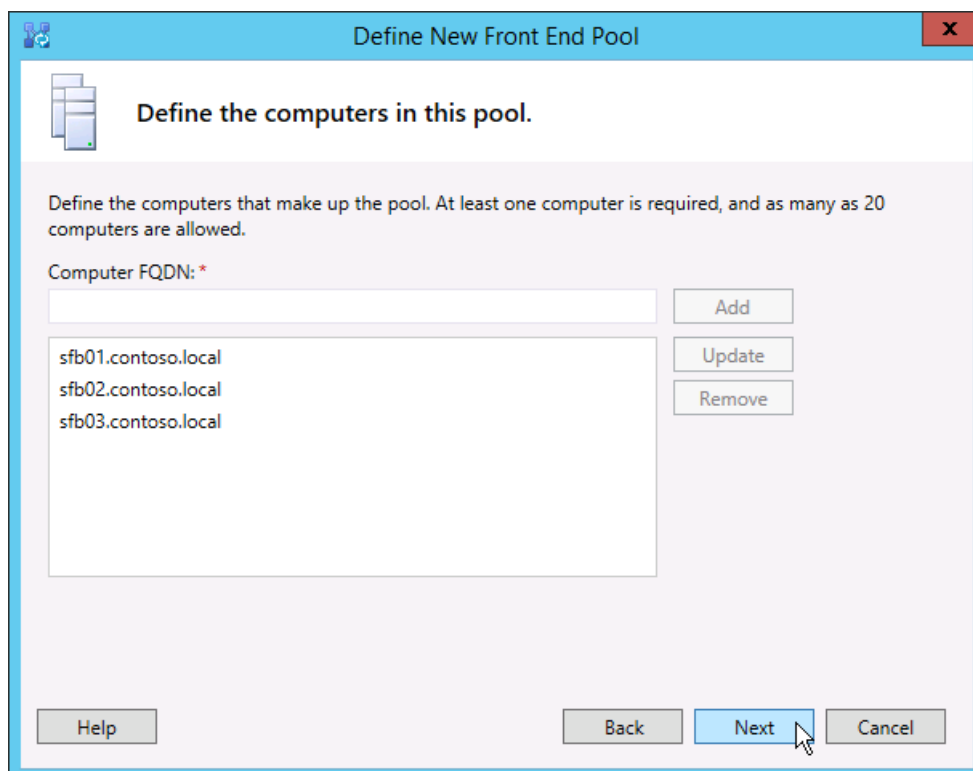
#### **TIP**

Skype for Business Server Enterprise Edition can include multiple servers working together to provide the Front End role. When multiple servers are used to fulfill the role, it is called a pool. Thus, multiple servers working together to provide the Front End role is also referred to as the Front End pool. Skype for Business Server Standard Edition can include only a single server to provide the Front End role. It is common to refer to the Front End pool even if only a single server is providing the role.





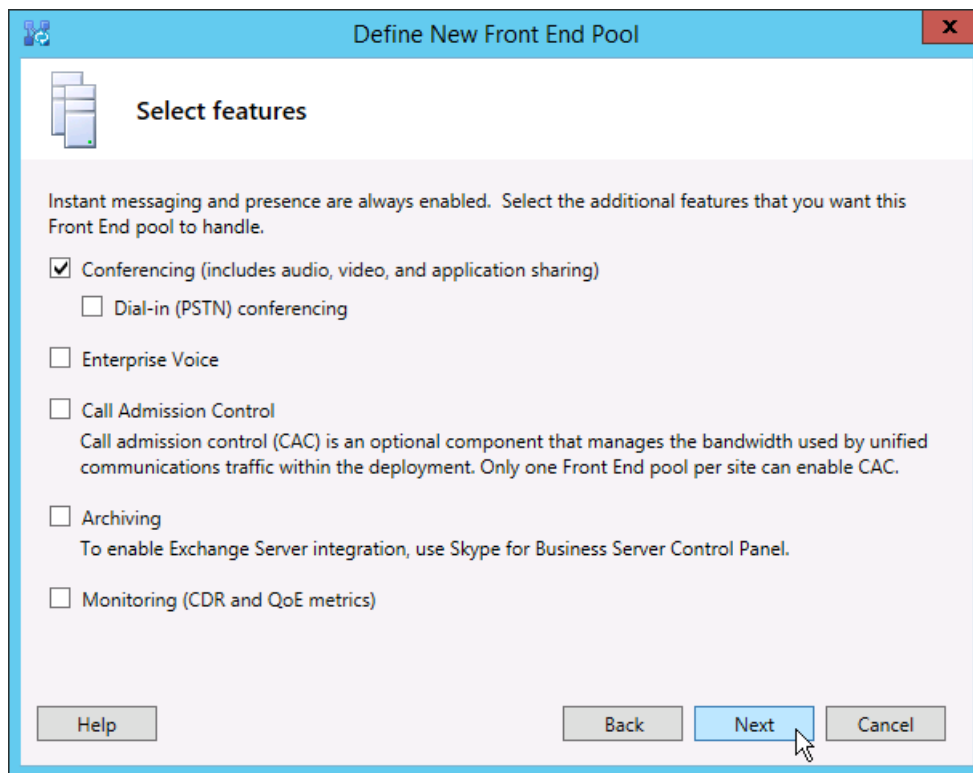
3. Enter the fully qualified domain names (FQDNs) of all computers in the pool, and then click **Next** as shown in the figure.



4. Select the features that will be included in this topology, and then click **Next** as shown in the figure.

**NOTE**

Skype for Business Server includes many advanced features. Review planning and deployment documentation for each specific feature you want to use.



5. On the **Select collocated server roles** page, you can choose to collocate the Mediation server on the Front End server, or you can choose to deploy it as a standalone server.

If you intend to collocate the Mediation server on the Enterprise Edition Front End pool, ensure the check box is selected. The server role will be deployed on the pool servers. If you intend to deploy the Mediation server as a stand-alone server, clear the appropriate check box. You will deploy the Mediation server in a separate deployment step after you completely deploy the Front End server. For planning details about a collocation, see [Topology Basics for Skype for Business Server](#).

6. By using the **Associate server roles with this Front End pool** page, you can define and associate server roles with the Front End pool. The following role is available:

**Enable an Edge pool** Defines and associates a single Edge Server or a pool of Edge Servers. An Edge Server facilitates communication and collaboration between users inside the organization and people outside the organization, including federated users.

There are two possible scenarios that you can use to deploy and associate the server roles.

For scenario one, you are defining a new topology for a new installation. You can approach the installation in one of the two following ways:

- Leave the check box clear, and define the topology. After you have published, configured, and tested the Front End and Back End Server roles, you can run Topology Builder again to add the role servers to the topology. By using this strategy, you can test the Front End pool and the server running SQL Server without additional complications from additional roles. After you have completed your initial testing, you can run Topology Builder again to select the roles you need to deploy.
- Select roles that you need to install, and then set up the hardware to accommodate the selected roles.

For scenario two, you have an existing deployment, and your infrastructure is ready for new roles, or you need to associate existing roles with a new Front End server.

- In this case, you will select the roles that you intend to deploy or associate with the new Front End server. In either case, you will proceed with the definition of the roles, set up any needed hardware, and proceed with the installation.

7. Next, you will define the SQL Server store that will be used with the topology. In this example, we use the Default instance. For more information about SQL Server features, such as High Availability, see [Plan for high availability and disaster recovery in Skype for Business Server](#).

- To use an existing SQL Server store that has already been defined in your topology, select an instance from **SQL store**.
- To define a new SQL Server instance to store pool information, click **New**, and then specify the **SQL Server FQDN** in the **Define New SQL Store** dialog box.
- To specify the name of a SQL Server instance, select **Named Instance**, and then specify the name of the instance.
- To use the default instance, click **Default instance**.
- To use SQL Mirroring, select **Enable SQL mirroring**, and select an existing instance, or create a new instance.

#### NOTE

SQL Mirroring is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering methods are preferred with Skype for Business Server 2019.

For this example, we enter the **SQL Server FQDN**, and configure any relevant high availability settings, and then click **OK**, as shown in the figure.

Define New Front End Pool

### Define the SQL Server store

Select existing or define a new SQL Server instance to store user information. For this Enterprise Edition Front End pool, the SQL Server instance cannot be collocated on the pool. It must be on a single-server pool. Note: SQL Server must be installed, and the SQL instance must be created before installation.

SQL Server store:

sql.contoso.local\Default

Enable SQL Server store mirroring

Mirroring SQL Server store:

Use SQL Server mirroring witness to enable automatic failover

8. Decide if you want to enable SQL Server store mirroring or SQL Server mirroring witness, and then click **Next**.

9. Define the file share that you want to use.

- To use a file share that has already been defined in your topology, select **Use a previously defined file share**.
- To define a new file share, select **Define a new file share**, in the **File Server FQDN** box, enter the

FQDN of the existing file server where the file share is to reside, and then enter a name for the file share in the **File Share** box.

For this example, we will click **Define a new file store**, enter the **file server FQDN** and **file share**, and then click **Next**.

#### NOTE

The file share for Skype for Business Server can be collocated but it is not recommended for performance reasons. Note that in this example, the file share has been located on a single dedicated server that will act as the file share. However, other more robust file share systems, such as DFS using Windows Server 2012 R2, are recommended. For details about supported file share systems, see [Requirements for your Skype for Business environment](#). For more information about creating the file share, see [Create a file share in Skype for Business Server](#). You can define the file share without the file share having been created. You will need to create the file share in the location you define before you publish the topology.

10. On the Specify the Web Services URL page, you must decide if you need to override the internal Web Services pool base URL. The reason for this override has to do with load balancing. Basic SIP traffic can be load balanced through simple DNS load balancing. However, the HTTP/S Web Services network traffic must use a supported Hardware or Software load balancing solution. For supported load balancers, see [Infrastructure for Skype for Business](#). In this example, we used DNS load balancing for SIP traffic and a supported software load balancing solution. Because we are dividing the traffic this way, we need to override the internal Web Services pool FQDN. Alternatively, if we had a top line load balancer and sent all traffic through it instead of using DNS load balancing for SIP traffic, we would not need to override the Web Services URL.

In the DNS section of this topic, we created an A record for webint.contoso.local. This is the URL we are using for the web services HTTP/S traffic, and it must go through the supported software load balancer we set up. Therefore, in this example, we override the URL to let Skype for Business Server know that all HTTP/S traffic should go to webint.contoso.local instead of pool.contoso.local, as shown in the figure. For more about load balancing, see [Load balancing requirements for Skype for Business](#).

#### IMPORTANT

The base URL is the Web Services identity for the URL, minus the https://. For example, if the full URL for the Web Services of the pool is <https://webint.contoso.local>, the base URL is webint.contoso.local.

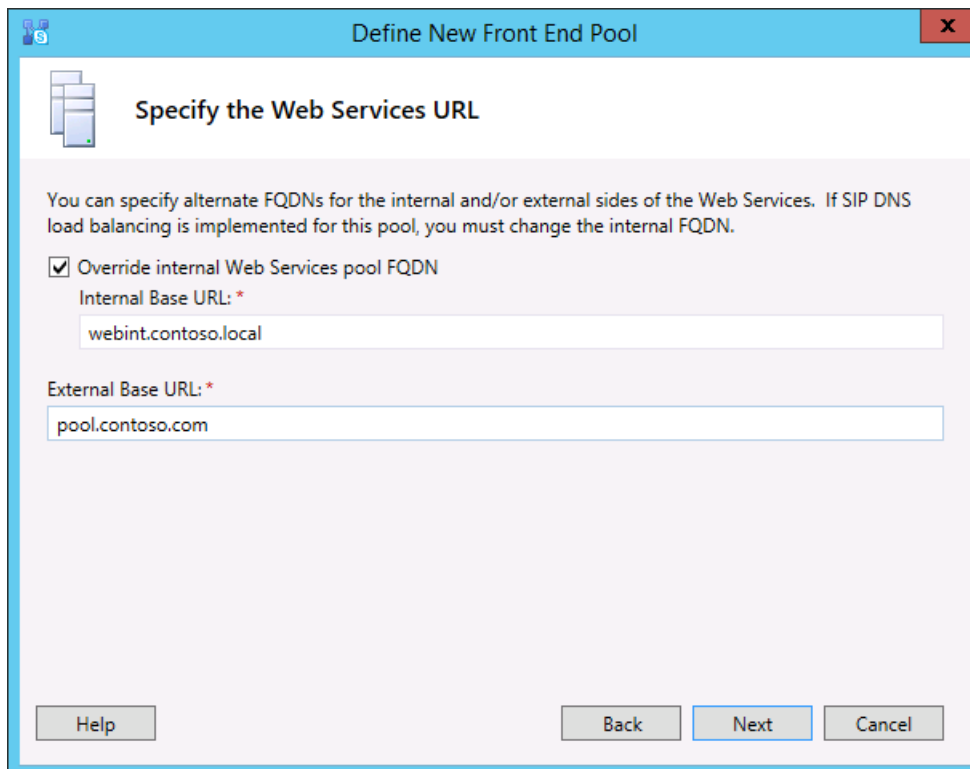
- If you are configuring DNS load balancing, as we are in this example, select the **Override internal Web Services pool FQDN** check box, and enter the internal base URL (which must be different from the pool FQDN) in **Internal Base URL**.

#### Caution

If you decide to override the Internal Web Services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director, or Director pool. **Use only standard characters** (including A-Z, a-z, 0-9, and hyphens) when you define URLs or fully qualified domain names. Do not use Unicode characters or underscores. Nonstandard characters in a URL or FQDN are often not supported by external DNS and public certification authorities (CAs) (that is, when the URL or FQDN must be assigned to the subject name or subject alternative name in the certificate).

- Optionally, enter the external base URL in **External Base URL**. You would enter the external base URL to differentiate it from your internal domain name. For example, your internal domain is contoso.local, but your external domain name is contoso.com. You would define the URL using the contoso.com domain name since it must be resolvable from public DNS. This is also important in the case of a reverse proxy. The external base URL domain name would be the same as the domain name of the FQDN of the reverse proxy. HTTP access to the Front End pool is required for instant

messaging and presence on mobile clients.



The screenshot shows a dialog box titled "Define New Front End Pool" with a close button (X) in the top right corner. The main heading is "Specify the Web Services URL". Below the heading is a paragraph: "You can specify alternate FQDNs for the internal and/or external sides of the Web Services. If SIP DNS load balancing is implemented for this pool, you must change the internal FQDN." There is a checked checkbox labeled "Override internal Web Services pool FQDN". Below this checkbox are two text input fields: "Internal Base URL: \*" containing "webint.contoso.local" and "External Base URL: \*" containing "pool.contoso.com". At the bottom of the dialog are four buttons: "Help", "Back", "Next", and "Cancel".

11. If you selected **Conferencing** on the **Select Features** page, you will be asked to select an Office Web Apps server. Click **New** to launch the dialog box.
12. In the **Define New Office Web Apps Server** dialog box, type the FQDN of your Office Web Apps server in the **Office Web Apps Server FQDN** box; when you do this, your Office Web Apps server discovery URL should automatically be entered into the **Office Web Apps Server discovery URL** box.

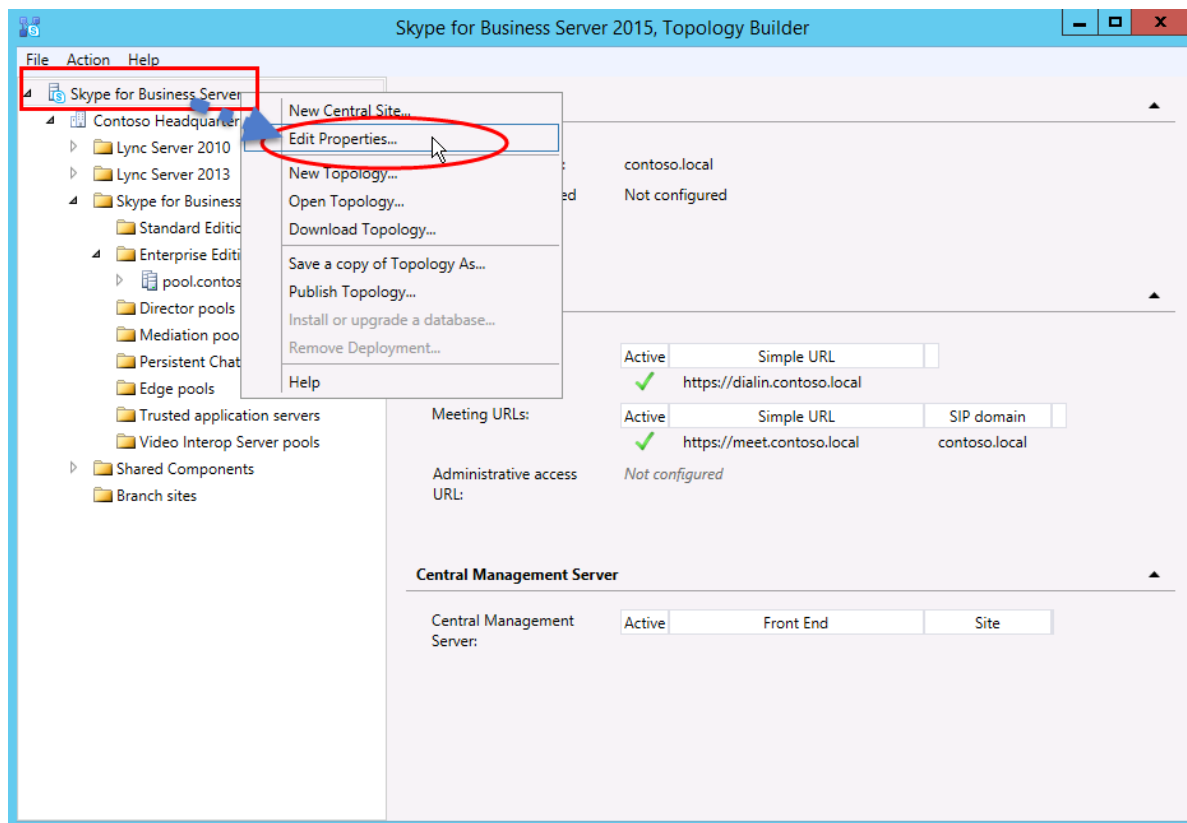
If the Office Web Apps server is installed on-premises and in the same network zone as Skype for Business Server, do not select the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)**.

If the Office Web Apps server is deployed outside your internal firewall, select the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)**.

13. Click **Finish** to complete the configuration. If you defined other role servers on the **Associate server roles with this Front End pool** page, separate role configuration wizard pages will open where you can configure the server roles. In this example we only chose conferencing.

### Configure simple URLs

1. In Topology Builder, right-click the **Skype for Business Server** top node, and then click **Edit Properties**, as shown in the figure.



2. In the **Simple URLs** pane, select either **Phone access URLs:** (Dial-in) or **Meeting URLs:** (Meet) to edit, and then click **Edit URL**.
3. Update the URL to the value you want, and then click **OK** to save the edited URL. You should configure the simple URL using the external SIP domain so that external users can join meetings, for example, contoso.com, which is external, as opposed to contoso.local, which is an internal domain. Thus, the SIP domain should be able to be resolved by external DNS.
4. Edit the Meet URL by using the same steps, if necessary.

#### To define the optional Admin simple URL

1. In Topology Builder, right-click the **Skype for Business Server** node, and then click **Edit Properties**.
2. In the **Administrative access URL** box, enter the simple URL you want for administrative access to Skype for Business Server Control Panel, and then click **OK**.

#### TIP

We recommend using the simplest possible URL for the Admin URL. The simplest option is `https://admin.<domain>`. The Admin URL can be either an internal or external domain, for example, contoso.local or contoso.com, as long as either record is resolvable in internal DNS.

#### IMPORTANT

If you change a simple URL after initial deployment, you must be aware of what changes impact your Domain Name System (DNS) records and certificates for simple URLs. If the change impacts the base of a simple URL, you must change the DNS records and certificates, too. For example, changing from `https://sfb.contoso.com/Meet` to `https://meet.contoso.com` changes the base URL from sfb.contoso.com to meet.contoso.com, so you would need to change the DNS records and certificates to refer to meet.contoso.com. If you changed the simple URL from `https://sfb.contoso.com/Meet` to `https://sfb.contoso.com/Meetings`, the base URL of sfb.contoso.com stays the same, so no DNS or certificate changes are needed. Whenever you change a simple URL name, however, you must run the **Enable-CsComputer** cmdlet on each Director and Front End server to register the change.

## Publish and verify the topology

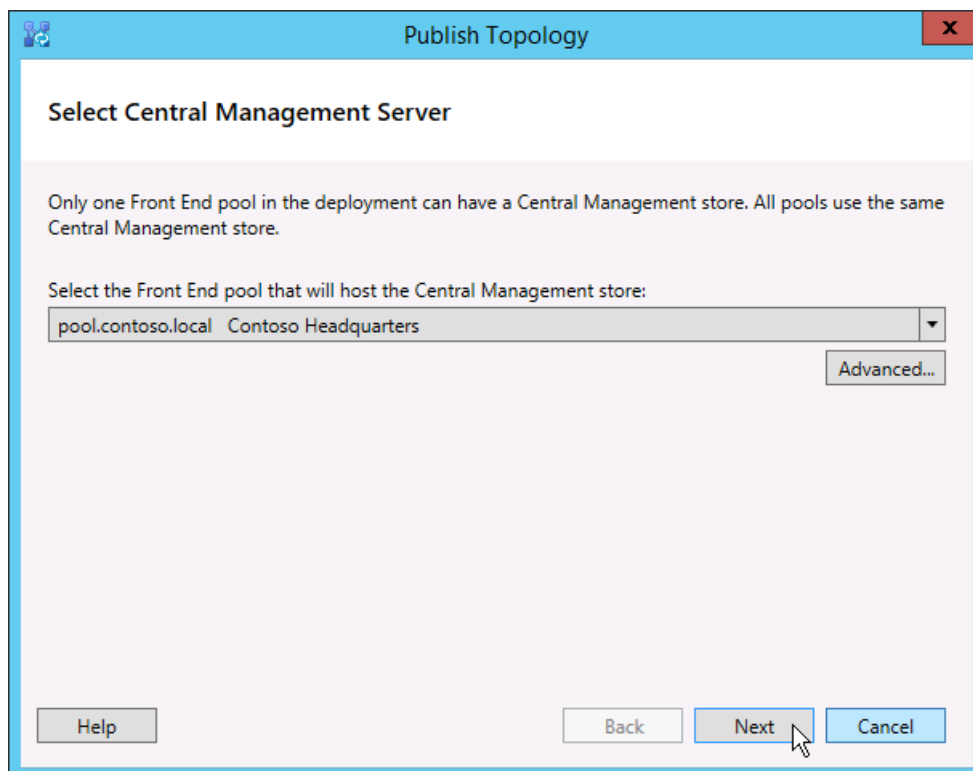
1. Check that all simple URLs are configured correctly.
2. Confirm that the SQL Server-based server is online and available to the computer where Topology Builder is installed, including any necessary firewall rules.
3. Confirm that the file share is available and that the proper permissions are defined.
4. Confirm that the correct server roles that meet the deployment requirements are defined in the topology.
5. Verify that the servers exist in Active Directory Domain Services (AD DS). This happens automatically when you join the servers to the domain.

When you have verified the topology and there are no validation errors, you should be ready to publish the topology. If there are validation errors, you must correct them before you can publish the topology.

6. Right-click the **Skype for Business Server** node, and then click **Publish Topology**.
7. On the **Publish the topology** page, click **Next**.
8. On the **Select Central Management Server** page, select a Front End pool, as shown in the figure.

### NOTE

You can click **Advanced** to configure database file locations.



9. On the **Select databases** page, select the databases you want to publish.

### NOTE

If you don't have the appropriate rights to create the databases, you can clear the check boxes next to those databases, and someone with appropriate rights can later create the databases. For details about requirements, see [Server requirements for Skype for Business Server](#).

10. Optionally click **Advanced**. By using Advanced SQL Server data file placement options, you can select

between the following options:

- **Automatically determine database file location** - This option determines the best operational performance based on the disk configuration on your SQL Server-based server by distributing the log and data files to the best location.
- **Use SQL Server instance defaults** - This option puts log and data files onto the SQL Server-based server by using the instance settings. This option does not use the operational functionality of the SQL Server-based server to determine optimal locations for logs and data. The SQL Server administrator would typically move the log and data files to locations that are appropriate for the SQL Server-based server and organization management procedures.

Click **OK**, and then click **Next**.

11. Optionally, click **Advanced**. By using Advanced SQL Server data file placement options, you can select between the following options:

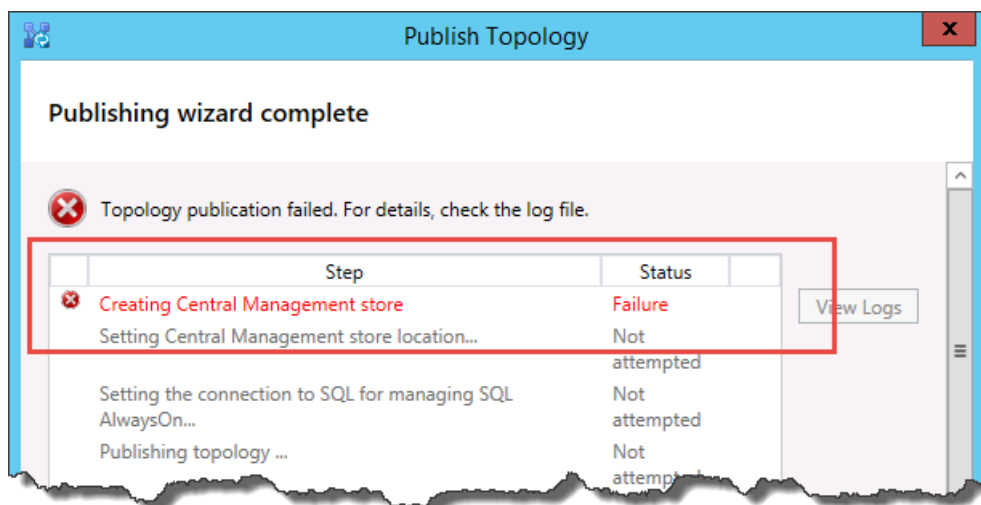
- **Automatically determine database file location** - This option determines the best operational performance based on the disk configuration on your SQL Server-based server by distributing the log and data files to the best location.
- **Use SQL Server instance defaults** - This option puts log and data files onto the SQL Server-based server by using the instance settings. This option does not use the operational functionality of the SQL Server-based server to determine optimal locations for logs and data. The SQL Server administrator would typically move the log and data files to locations that are appropriate for the SQL Server-based server and organization management procedures.

Click **OK**.

12. Click **Next** to complete the publishing process.

#### NOTE

A common failure for this step is that the SQL Server databases cannot be created. When the process cannot complete, an error is provided, as shown in the figure. The most likely cause is that the user attempting to create the database does not have the appropriate permissions, or the SQL Server system cannot be contacted due to a firewall or other network issue.



13. When the publishing process completes, you are presented with a link to open a list of next steps. Click **Click here to open to-do list** to view the next steps, and then click **Finish**.

The "Completed with warnings" message for the database creation does not mean there was an error. The



installation process has to change settings in SQL Server for Skype for Business Server to work correctly. When a setting is changed in SQL Server, it is logged as a warning so that SQL Server administrators can understand exactly what the installation process completed. If you receive a warning, you can select the record, and then click **View Logs** to view the details of the warning.

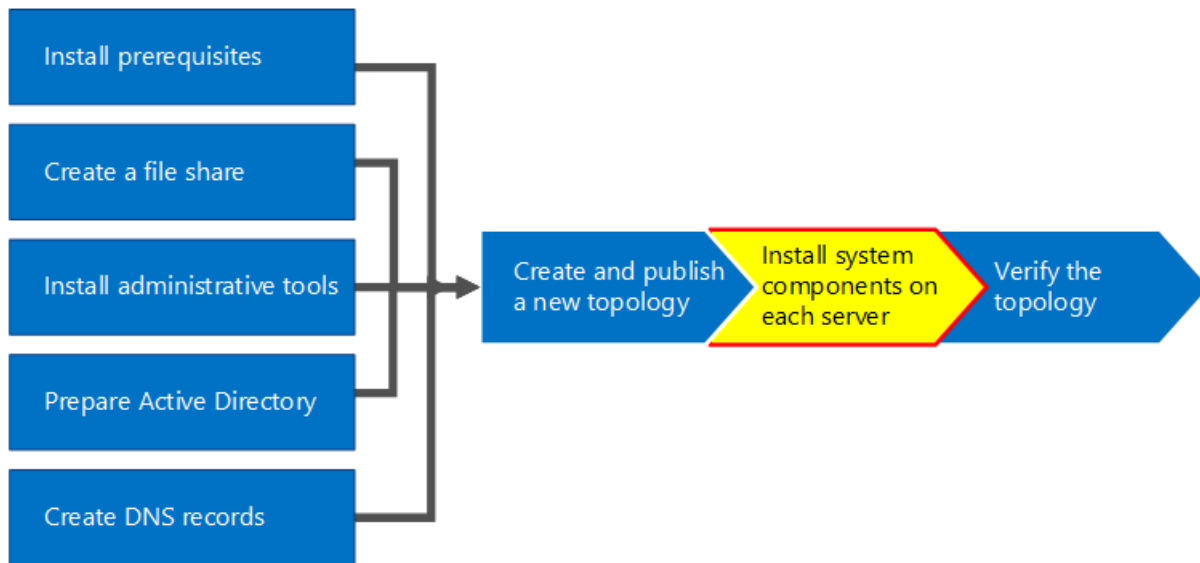
When the topology has been successfully published, you can begin installing a local replica of the Central Management store on each server running Skype for Business Server in your topology. We recommend that you begin with the first Front End pool.

# Install Skype for Business Server on servers in the topology

8/7/2019 • 13 minutes to read

**Summary:** Learn how to install the Skype for Business Server system components on each server in the topology. Download a free trial of Skype for Business Server from the [Microsoft Evaluation center](#).

Once the topology is loaded into the Central Management Store and Active Directory knows which servers will perform which roles, you need to install the Skype for Business Server system on each of the servers in the topology. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5 as outlined in the diagram. Installing the Skype for Business Server system is step 7 of 8.



## Install Skype for Business Server system

Once you have published a topology, you can install the Skype for Business Server components on each server in the topology. This section guides you through installing Skype for Business Server and setting up the server roles for the Front End pool and any server roles that are collocated with the Front End servers. To install and set up server roles, you run the Skype for Business Server Deployment Wizard on each computer on which you are installing a server role. You use the Deployment Wizard to complete all four deployment steps, including installing the Local Configuration store, installing the Front End Servers, configuring certificates, and starting services.

### IMPORTANT

You must use Topology Builder to complete and publish the topology before you can install Skype for Business Server on servers.

### NOTE

This procedure must be completed for all servers in the topology.

### Caution

After you install Skype for Business Server on a Front End Server, the first time you start services, you must make sure that the Windows Firewall Service is running on the server.

**Caution**

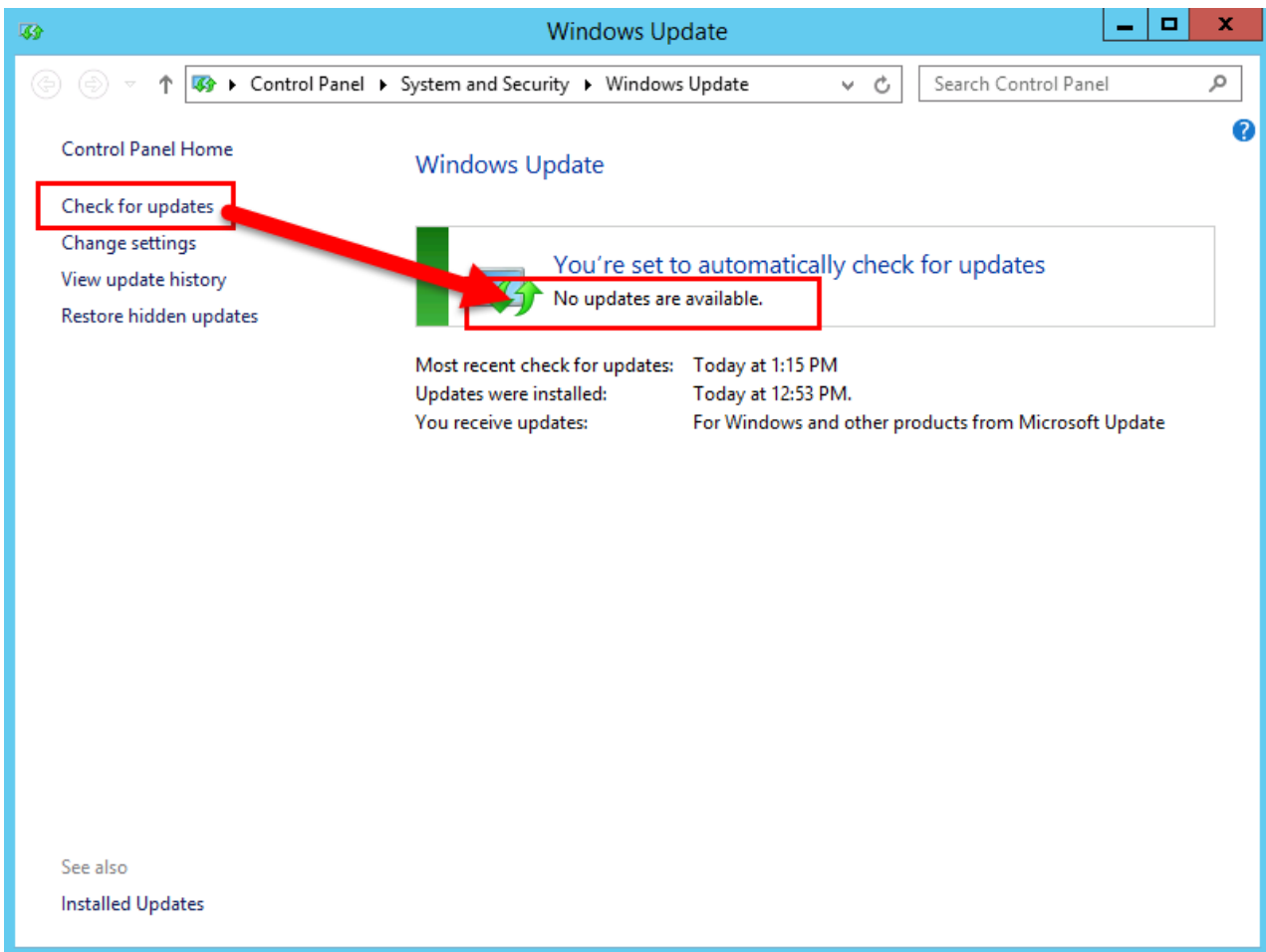
Before you follow these steps, make sure you're logged onto the server with a domain user account that's both a local administrator and a member of the RTCUniversalServerAdmins group.

**NOTE**

If you haven't run Skype for Business Server setup on this server before, you'll be prompted for a drive and path for the installation. This provides the capability to install to a drive other than the system drive, if your organization requires it, or if you have space concerns. You can change the installation location path for the Skype for Business Server files in the **Setup** dialog box to a new, available drive. If you install the Setup files to this path, including OCSCore.msi, the rest of the Skype for Business Server files will deploy there as well.

**IMPORTANT**

Before you begin the installation, make sure that Windows Server is up-to-date by using Windows Update.



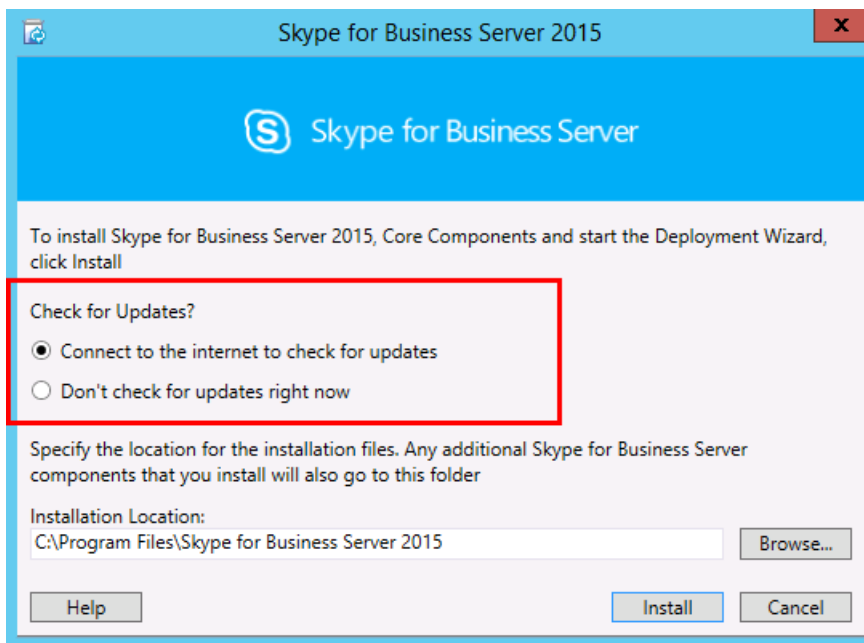
**Install Skype for Business Server system**

1. Insert the Skype for Business Server installation media. If the setup does not automatically begin, double-click **Setup**.
2. The installation media requires Microsoft Visual C++ to run. A dialog will pop up asking if you want to install it. Click **Yes**.
3. Carefully review the License Agreement, and if you agree, select **I accept the terms in the license agreement**, and click **OK**.
4. Smart Setup is a feature in Skype for Business Server where you can connect to the Internet to check for updates from Microsoft Update (MU) during the installation process, as shown in the figure. This provides a

better experience by making sure you have the most recent updates for the product. Click **Install** to begin the installation.

#### NOTE

Many organizations have Windows Server Update Services (WSUS) deployed in their corporate environments. WSUS lets administrators fully manage the distribution of updates that are released through Microsoft Update to computers in their network. As part of the Cumulative Update 1 release Skype for Business Server introduced support for Smart Setup to work with WSUS. Customers with WSUS who are deploying Skype for Business Server for the first time or upgrading from the Lync Server 2013 environment using the In-Place Upgrade feature will have Smart Setup fetching Skype for Windows updates from WSUS as opposed to fetching updates from MU. Customers wanting to use Smart Setup need to run the SmartSetupWithWSUS.psq on all the machines before running Setup.exe.



5. On the Deployment Wizard page, click **Install or Update Skype for Business Server System**.
6. Perform the procedures in the following procedures, when you've completed them, click **Exit** to close the Deployment Wizard. Repeat the procedures for each Front End server in the pool.

#### Step 1: Install Local Configuration Store

1. Review the prerequisites, and then click **Run** next to **Step 1: Install Local Configuration Store**.

#### NOTE

The Local Configuration Store is a read-only copy of the Central Management Store. In a Standard Edition deployment, the Central Management Store is created using a local copy of SQL Server Express Edition on the Front End server. This happens when you run the Prepare First Standard Edition Server procedure. In an Enterprise Edition deployment, the Central Management store is created when you publish the topology that includes an Enterprise Edition Front End pool.

2. On the **Install Local Configuration Store** page, make sure that the **Retrieve directly from the Central Management store** option is selected, and then click **Next**.

SQL Server Express Edition is installed on the local server. SQL Server Express Edition is required for the local configuration store.

3. When the local server configuration installation is complete, click **Finish**.

## Step 2: Setup or remove Skype for Business Server components

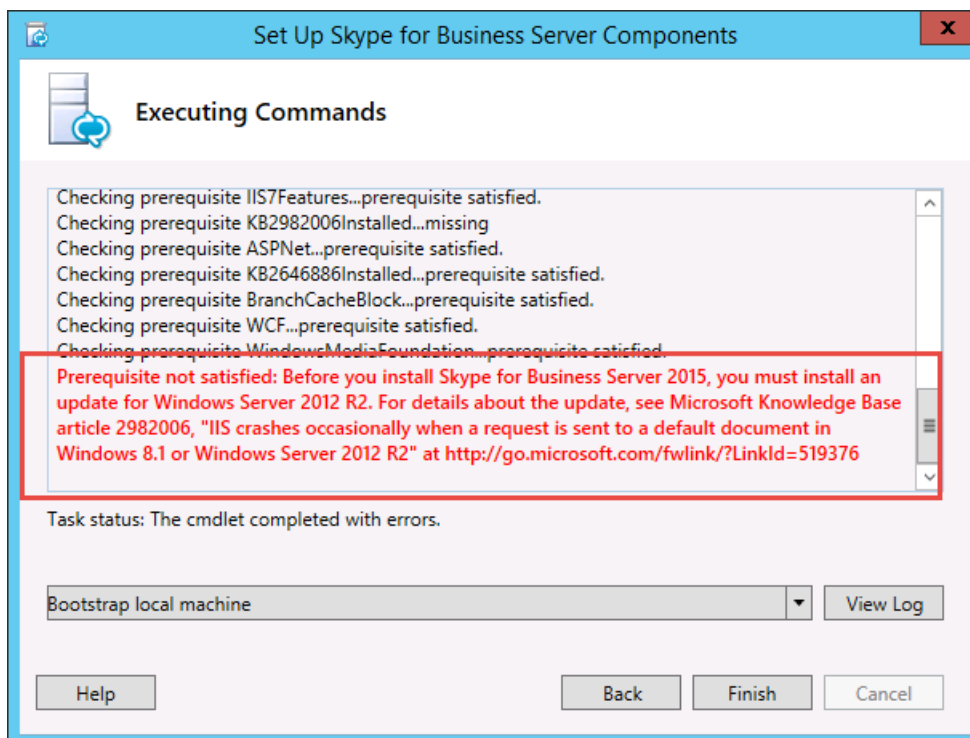
1. Review the prerequisites, and then click **Run** next to **Step 2: Setup or Remove Skype for Business Server Components**.
2. On the **Set Up Skype for Business Server Components** page, click **Next** to set up components as defined in your published topology.
3. The **Executing Commands** page displays a summary of commands and installation information as the set up takes place. When it's done, you can use the list to select a log to view, and then click **View Log**.
4. When Skype for Business Server components setup is done and you've reviewed the logs as needed, click **Finish** to complete this step in the installation.

### NOTE

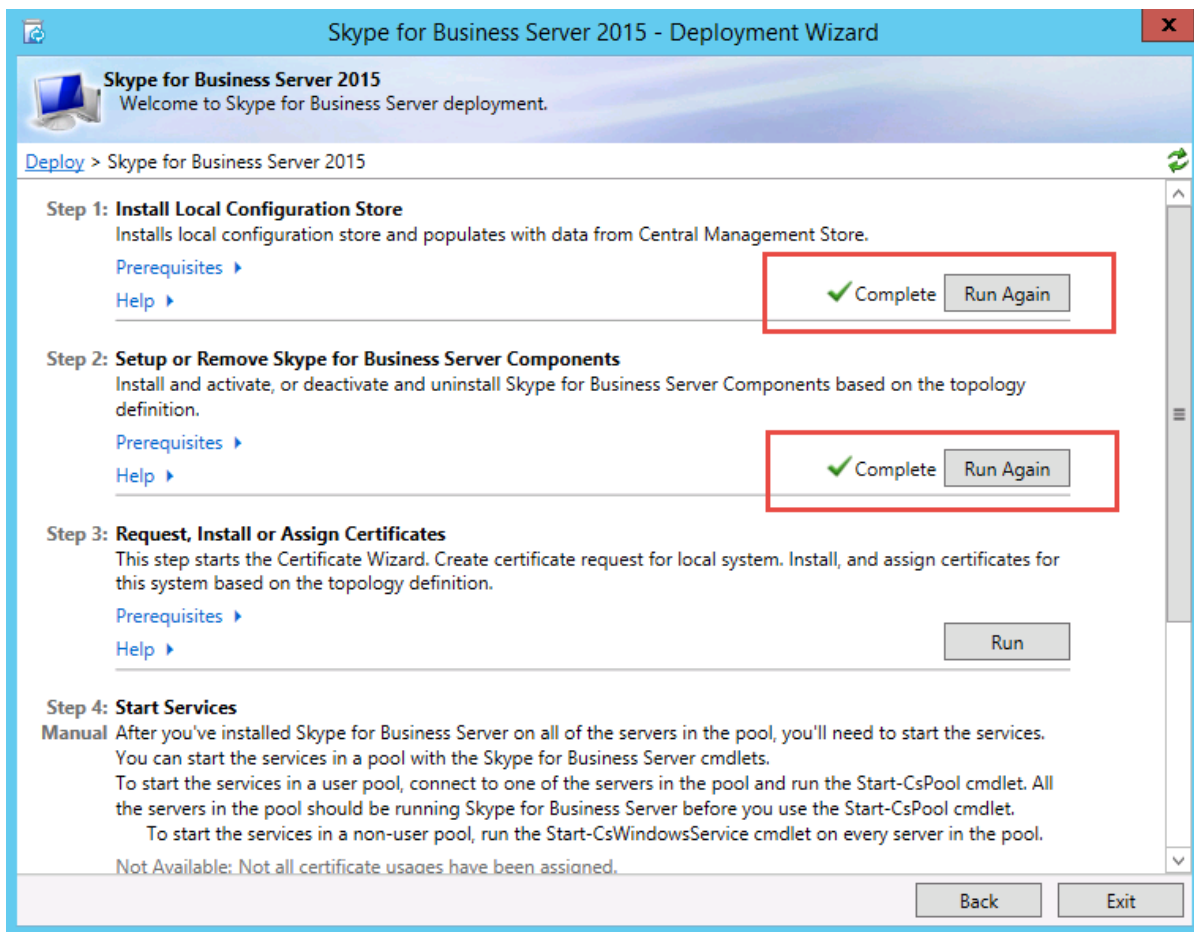
Restart the server if prompted (which might happen if Windows Desktop Experience needed to be installed). When the computer is back up and running, you need to run this (Step 2: Setup or Remove Skype for Business Server Components) procedure again.

### NOTE

If the installer finds any prerequisites that have not been satisfied, you will be notified with a "Prerequisite not satisfied" message, as shown in the figure. Satisfy the required prerequisite, and then start this (Step 2: Setup or Remove Skype for Business Server Components) procedure again.



5. Verify that the first two steps completed as expected. Confirm that there is a green checkmark with the word **Complete**, as shown in the figure.



6. Run **Windows Update** again to check if there are any updates after you install the Skype for Business Server Components.

### Step 3: Request, install, or assign certificates

1. Review the prerequisites, and then click **Run** next to **Step 3: Request, Install or Assign Certificates**.

#### NOTE

Skype for Business Server includes support for the SHA-2 suite (SHA-2 uses digest lengths of 224, 256, 384 or 512 bits) of digest hash and signing algorithms for connections from clients running the Windows 10, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 operating systems. To support external access using the SHA-2 suite, the external certificate is issued by a public CA that also can issue a certificate with the same bit length digest.

#### IMPORTANT

The selection of which hash digest and signing algorithm is dependent on the clients and the servers that will use the certificate, and other computers and devices that clients and servers will communicate with who must also know how to use the algorithms used in the certificate. For information on which digest lengths are supported in the operating system and some client applications, see [Windows PKI blog - SHA2 and Windows](#).

Each Standard Edition or Front End server requires up to four certificates: the oAuthTokenIssuer certificate, a default certificate, a web internal certificate, and a web external certificate. However, you can request and assign a single default certificate with appropriate subject alternative name entries as well as the oAuthTokenIssuer certificate. For details about the certificate requirements, see [Environmental requirements for Skype for Business Server](#) or [Server requirements for Skype for Business Server 2019](#).

### IMPORTANT

The following procedure describes how to configure certificates from an internal Active Directory Certificate Services based certificate authority.

2. On the **Certificate Wizard** page, click **Request**.
3. On the **Certificate Request** page fill in the relevant data including selecting the SIP domain and , click **Next**.
4. On the **Delayed or Immediate Requests** page, you can accept the default **Send the request immediately to an online certification authority** option by clicking **Next**. The internal CA with automatic online enrollment must be available if you select this option. If you choose the option to delay the request, you will be prompted for a name and location to save the certificate request file. The certificate request must be presented and processed by a CA either inside your organization, or by a public CA. You will then need to import the certificate response and assign it to the proper certificate role.
5. On the **Choose a Certificate Authority (CA)** page, select the **Select a CA from the list detected in your environment** option, and then select a known (through registration in Active Directory Domain Services) CA from the list. Or, select the **Specify another certification authority** option, enter the name of another CA in the box, and then click **Next**.
6. On the **Certificate Authority Account** page, you are prompted for credentials to request and process the certificate request at the CA. You should have determined if a user name and password is necessary to request a certificate in advance. Your CA administrator will have the required information and might have to assist you in this step. If you need to supply alternate credentials, select the check box, provide a user name and password in the text boxes, and then click **Next**.
7. On the **Specify Alternate Certificate Template** page, to use the default Web Server template, click **Next**.

### NOTE

If your organization has created a template for use as an alternative for the default Web server CA template, select the check box, and then enter the name of the alternate template. You will need the template name as defined by the CA administrator.

8. On the **Name and Security Settings** page, specify a **Friendly Name**. By using a friendly name, you can quickly identify the certificate and purpose. If you leave it blank, a name will be generated automatically. Set the **Bit length** of the key, or accept the default of 2048 bits. Select the **Mark the certificate's private key as exportable** if you determine that the certificate and private key needs to be moved or copied to other systems, and then click **Next**.

### NOTE

Skype for Business Server has minimal requirements for an exportable private key. One such place is on the Edge Servers in a pool, where the Media Relay Authentication Service uses copies of the certificate, rather than individual certificates for each instance in the pool.

9. On the **Organization Information** page, optionally provide organization information, and then click **Next**.
10. On the **Geographical Information** page, optionally provide geographical information, and then click **Next**.
11. On the **Subject Name / Subject Alternate Names** page, review the subject alternative names that will be

added, and then click **Next**.

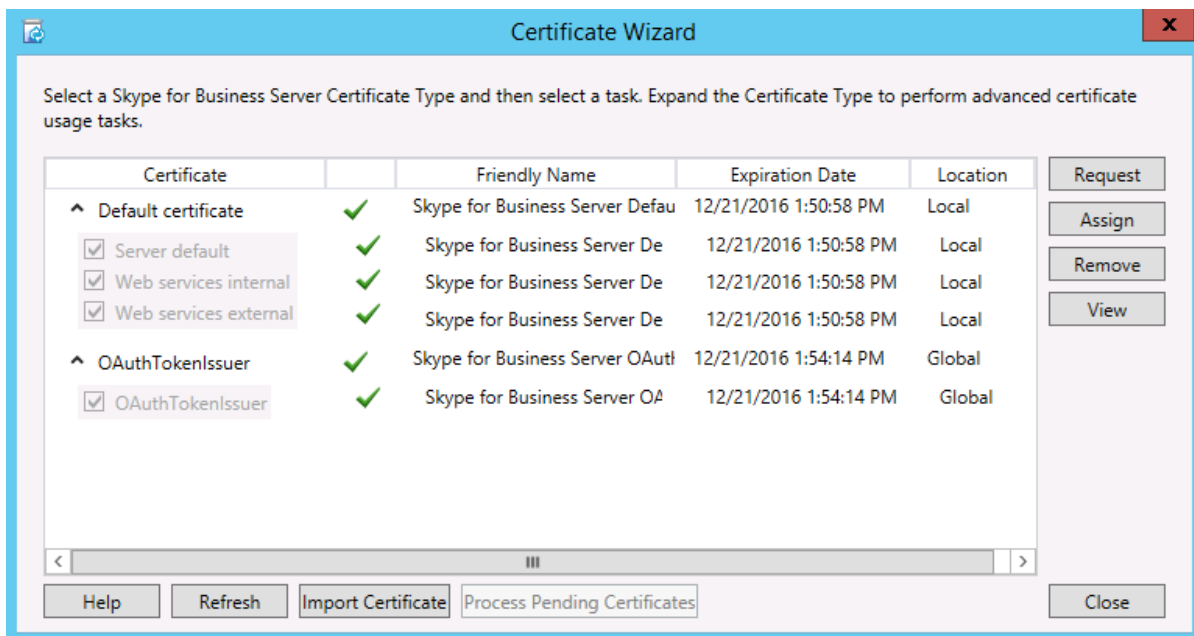
12. On the **SIP Domain setting** page, select the **SIP Domain**, and then click **Next**.
13. On the **Configure Additional Subject Alternate Names** page, add any additional required subject alternative names, including any that might be required for additional SIP domains in the future, and then click **Next**.
14. On the **Certificate Request Summary** page, review the information in the summary. If the information is correct, click **Next**. If you need to correct or modify a setting, click **Back** to the proper page to make the correction or modification.
15. On the **Executing Commands** page, click **Next**.
16. On the **Online Certificate Request Status** page, review the information returned. You should note that the certificate was issued and installed into the local certificate store. If it is reported as having been issued and installed, but it is not valid, make sure that the CA root certificate has been installed in the server's Trusted Root CA store. Refer to your CA documentation on how to retrieve a Trusted Root CA certificate. If you need to view the retrieved certificate, click **View Certificate Details**. By default, the check box for **Assign the certificate to Skype for Business Server certificate usages** is selected. If you want to manually assign the certificate, clear the check box, and then click **Finish**.
17. If you cleared the check box for **Assign the certificate to Skype for Business Server certificate usages** on the previous page, you will be presented with the **Certificate Assignment** page. Click **Next**.
18. On the **Certificate Store** page, select the certificate that you requested. If you want to view the certificate, click **View Certificate Details**, and then click **Next** to continue.

#### NOTE

If the **Online Certificate Request Status** page reported an issue with the certificate, such as the certificate is not valid, view the actual certificate for help in resolving the issue. Two specific issues that can cause a certificate to not be valid is the previously mentioned missing Trusted Root CA certificate, and a missing private key that is associated with the certificate. Refer to your CA documentation to resolve these two issues.

19. On the **Certificate Assignment Summary** page, review the information presented to make sure that this is the certificate that should be assigned, and then click **Next**.
20. On the **Executing Commands** page, review the output of the command. Click **View Log** if you want to review the assignment process or if there was an error or warning issued. When you are finished with your review, click **Finish**.
21. On the **Certificate Wizard** page, confirm that all services have a green check to indicate that all have been assigned a certificate, including the OAuthTokenIssuer ,as shown in the figure, and then click **Close**.





#### TIP

If you are installing in a lab environment and have just set up the Certificate Authority using Active Directory Certificate Services, you will need to reboot both the server running Certificate Services and also the Front End server before the certificate assignment can go through successfully.

#### TIP

For more information about certificates in Active Directory Certificate Services, see [Active Directory Certificate Services](#).

### Step 4: Start Services

1. Review the prerequisites for **Step 4: Start Services**.
2. If this is an Enterprise Edition Front End pool with at least three servers, Windows Fabric is used, and you must use the **Start-CsPool** cmdlet. If a single server is used, which is always the case with Standard Edition, you must use the **Start-CsWindowsService** cmdlet. In this example we are using Enterprise Edition with three Front End servers in the pool, open the **Skype for Business Server Management Shell** and run the **Start-CsPool** cmdlet as shown in the figure. For all other roles, including Standard Edition server, you must use **Start-CsWindowsService**. To deploy roles other than the Front End role, see documentation for those particular roles.

```

Administrator: Skype for Business Server Management Shell
PS C:\Users\administrator.CONTOSO> Start-CsPool

cmdlet Start-CsPool at command pipeline position 1
Supply values for the following parameters:
PoolFqdn: pool.contoso.local
Initializing...
Validating the pool Fqdn.
Pool Fqdn is valid.
Preparing the FrontEnd Server list ...
Done.
Preparing the Seed Nodes list ...
Done.
Starting the servers ...
Done.
Machine CONTOSO-SFB01.CONTOSO.LOCAL in Running state.
The state of each machine(s).
  Server Name : contoso-sfb01.contoso.local Status : Running

PS C:\Users\administrator.CONTOSO>

```

3. On the **Executing Commands** page, after all services have started successfully, click **Finish**.

**IMPORTANT**

The command to start the services on the server is a best effort method to report that the services have, in fact, started. It might not reflect the actual state of the service. We recommend that you use the step **Service Status (Optional)** to open the Microsoft Management Console (MMC) and confirm that the services have started successfully, as shown in the figure. If any Skype for Business Server service has not started, you can right-click that service in the MMC, and then click **Start**.

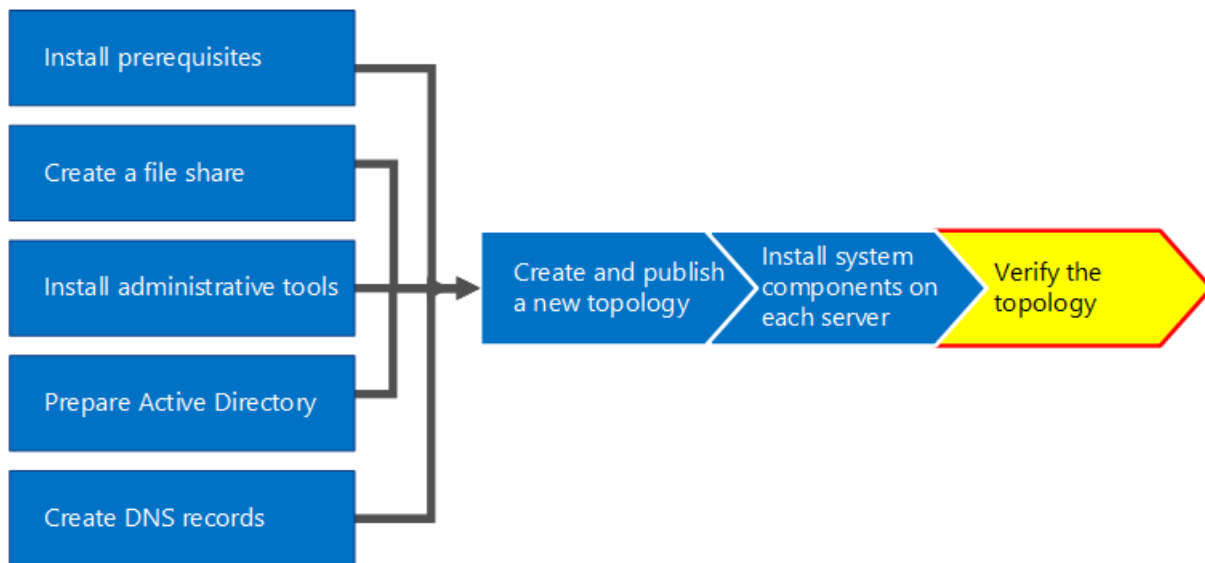
Server	Supports file, print, a...	Running	Automatic
Shell Hardware Detection	Provides notification...	Running	Automatic
Skype for Business Server Application Sharing	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Audio Test Service	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Audio/Video Conferen...	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Centralized Logging S...	Skype for Business S...	Running	Automatic (D...
Skype for Business Server File Transfer Agent	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Front-End	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Health Agent	Skype for Business S...	Running	Automatic (D...
Skype for Business Server IM Conferencing	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Master Replicator Agent	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Replica Replicator Agent	Skype for Business S...	Running	Automatic (D...
Skype for Business Server Web Conferencing	Skype for Business S...	Running	Automatic (D...
Skype for Business Server XMPP Translating Gat...	Skype for Business S...	Running	Automatic (D...
Smart Card	Manages access to s...	Disabled	Disabled
Smart Card Device Enumeration Service	Creates software dev...	Stopped	Manual (Trig...

# Verify the topology in Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Learn how to verify the Skype for Business Server topology and Active Directory servers are working as expected. Download a free trial of Skype for Business Server from the [Microsoft Evaluation center](#).

After you have the topology published and the Skype for Business Server system components installed on each of the servers in the topology, you are ready to verify that the topology is working as expected. This includes verifying that the configuration has propagated out to all of the Active Directory servers so that the entire domain knows Skype for Business is available in the domain. You can do steps 1 through 5 in any order. However, you must do steps 6, 7, and 8 in order, and after steps 1 through 5, as outlined in the diagram. Verifying the topology is step 8 of 8.



## Test the Front End pool deployment

The final step is to test the Front End pool and confirm that Skype for Business clients can communicate with each other.

### Add users and verify client connectivity

1. Use Active Directory Computers and Users to add the Active Directory user object of the administrator role for the Skype for Business Server deployment (on which Skype for Business Server Control Panel is installed) to the **CSAdministrator** group.

#### IMPORTANT

If you do not add the appropriate users and groups to the CsAdministrators group, you will receive an error when you open Skype for Business Server Control Panel which reads, "Unauthorized: Access is denied due to a role-based access control (RBAC) authorization failure."

2. If the user object is currently logged on, log off and then log on again to register the new group assignment.

#### NOTE

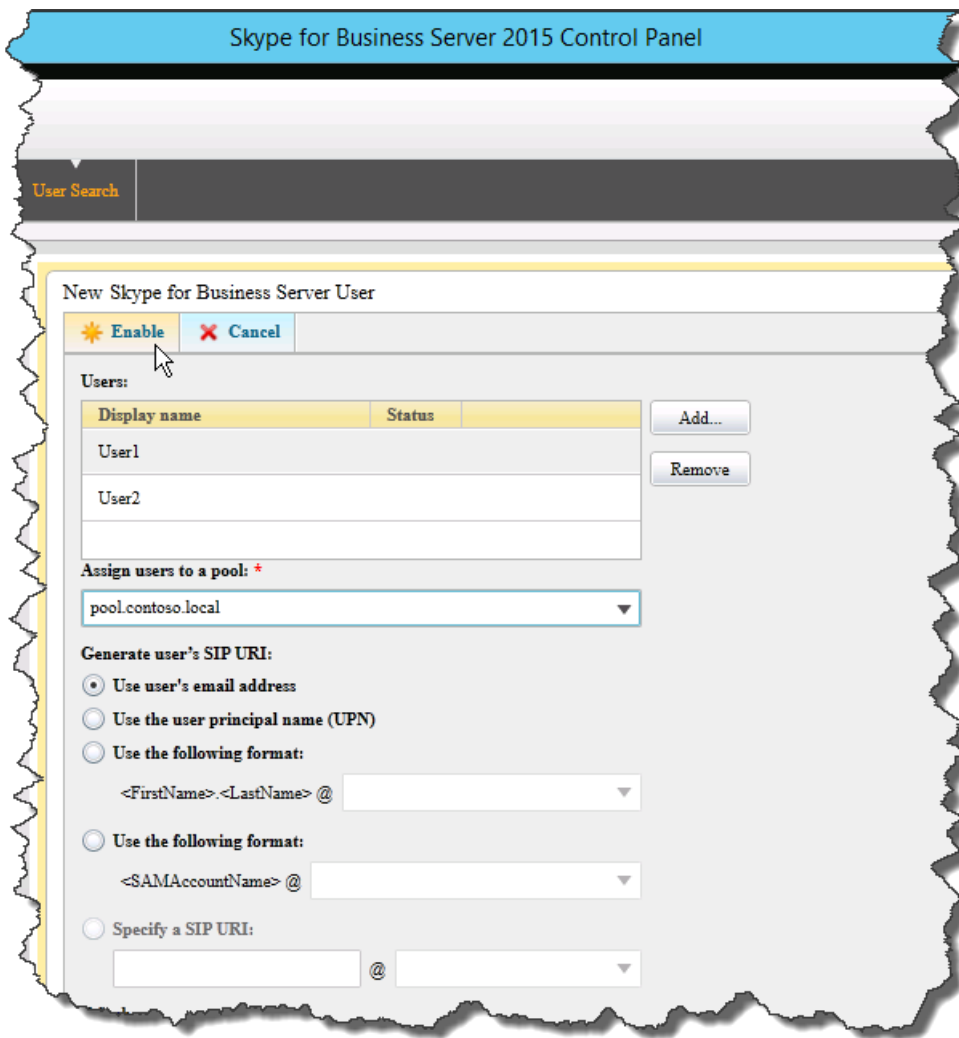
The user account cannot be the local administrator of any server running Skype for Business Server.

3. Use the administrative account to log on to the computer where Skype for Business Server Control Panel is installed.
4. Start Skype for Business Server Control Panel, and then provide credentials, if prompted. Skype for Business Server Control Panel displays deployment information.
5. In the left navigation bar, click **Topology**, and then confirm that the service status shows a computer with a green arrow and that a green check mark for replication status is next to each Skype for Business Server role that has been deployed and brought online.
6. In the left navigation bar, click **Users**, and then click **Enable users**.
7. On the **New Skype for Business Server User** page, click **Add**.
8. To define search parameters for the objects you want to find, on the **Select from Active Directory** page, you can select **Search**, and then optionally click **Add Filter**. You can also select **LDAP search** and enter an LDAP expression to filter or limit the objects that will be returned. After you have decided on your Search options, click **Find**.
9. In the Search results pane, select the users you want to add, and then click **OK**.
10. On the **New Skype for Business Server User** page, the users you selected are in the **Users** display. In the **Assign users to a pool** list, select the server where the users should reside.

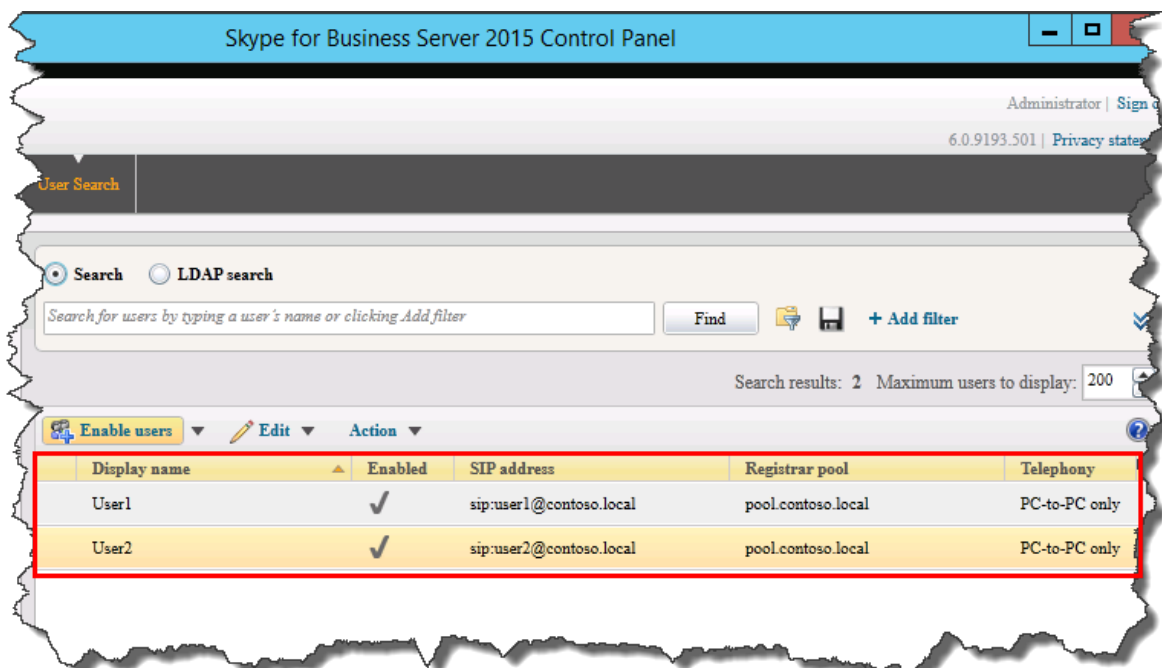
The following is a list of options you can use to configure the objects.

- **Generate user's SIP URI**
- **Telephony**
- **Line URI**
- **Conferencing policy**
- **Client version policy**
- **PIN policy**
- **External access policy**
- **Archiving policy**
- **Location policy**
- **Client policy**

To test the basic functionality, select the option you prefer for the **Generate user's SIP URI** setting (the other options in the configuration use default settings), and then click **Enable**, as shown in the figure.



11. A summary page is displayed that shows a check mark in the **Enabled** column to indicate that the users are setup. The **SIP address** column displays the address you need for the user sign-in configuration.



12. Log one user on to a computer that is joined to the domain and another user on to another computer in the domain.
13. Install Skype for Business client on each of the two client computers, and then verify that both users can sign in to Skype for Business Server and can send instant messages to each other.



# Deploy Call Via Work in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to deploy Call Via Work in Skype for Business Server for some or all of your users.

Use these steps to deploy Call Via Work for your users. Planning considerations are discussed in [Plan for Call Via Work in Skype for Business Server](#). In previous versions of Lync Server remote call control was a feature which enabled users to control their PBX phones with Lync Server. In Skype for Business Server, this feature has been replaced with Call Via Work.

## Prerequisites for Call Via Work

Call Via Work uses Unified Communications Web API (UCWA), which is automatically installed on all Skype for Business Server Front End Servers. To enable users for Call Via Work, you must also have the following prerequisites in place:

- You must have a Mediation Server deployed, either as part of a Front End Server or as a standalone role. You must also deploy an IP-PBX gateway.
- All users who will be enabled for Call Via Work must have a Direct Inward Dialing (DID) on the PBX phone system.
- You must enable all Call Via Work users for Enterprise Voice. When you do this, you must configure the Skype for Business DID number for each user to the corresponding DID number for the corresponding PBX phone system.
- All users who will be using Call Via Work must have **Automatic Configuration** selected in their **Advanced Connections** option in their Skype for Business client. This enables the client to discover the UCWA URLs. **Automatic Configuration** is the default selection.
- For each Call Via Work user, enable call forwarding and simultaneous ringing.
- For each Call Via Work user, ensure that dial-in conferencing and conferencing dial-out are enabled. This enables these users to get into and out of Skype for Business conferences.
- Ensure that delegation, team call, and response group are disabled for every Call Via Work user.

## Deploy Call Via Work

After the prerequisites are in place, do the following:

- Create a global phone number for your deployment which Skype for Business displays on the PBX caller ID of users who are making Call Via Work calls.
- Create one or more Call Via Work policies
- Assign a Call Via Work policy to each user who will be enabled for Call Via Work

### Create the Call Via Work global phone number

- Type the following cmdlet

```
Set-CsRoutingConfiguration -CallViaWorkCallerId +<PhoneNumber>
```

For example, the following cmdlet sets the global phone number to 1-555-123-4567.

```
Set-CsRoutingConfiguration -CallViaWorkCallerId +15551234567
```

### Create a Call Via Work policy

- Type the following cmdlet

```
New-CsCallViaWorkPolicy [-Identity] <XdsIdentity> [-Tenant <guid>] [-Enabled <bool>] [-UseAdminCallbackNumber <bool>] [-AdminCallbackNumber <string>] [-InMemory] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]
```

For example, the following cmdlet creates a Call Via Work policy called ContosoUser1CvWP, requires the user to use an admin callback number, and sets that callback number to 1-555-789-1234.

```
New-CsCallViaWorkPolicy -Identity Tag:ContosoUser1CvWP -Enabled $true -UseAdminCallbackNumber $true -AdminCallbackNumber +15557891234
```

### Assign a Call Via Work policy to a user

- Type the following cmdlet

```
Grant-CsCallViaWorkPolicy -Identity <UserName> -PolicyName Tag:<PolicyName>
```

For example, the following cmdlet assigns the Call Via Work policy "ContosoUser1CvWP" to the user named **ContosoUser1**.

```
Grant-CsCallViaWorkPolicy -Identity ContosoUser1 -PolicyName Tag:ContosoUser1CvWP
```

## See also

[Plan for Call Via Work in Skype for Business Server](#)



# Deploy archiving for Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Read this topic to learn how to deploy archiving for Skype for Business Server.

Archiving is automatically installed on each Front End Server in your Skype for Business Server deployment, but you still need to perform initial setup and configuration steps before you can use it. Before you begin, be sure you are familiar with the concepts in [Plan for archiving in Skype for Business Server](#).

## Deployment checklist

How you set up archiving depends on which storage option you choose:

- If you use Microsoft Exchange integration for all users in your deployment, you don't need to configure Skype for Business Server archiving policies for your users. Instead, you configure Exchange In-Place Hold policies to support archiving for users homed on Exchange, with their mailboxes put on In-Place Hold. For details about configuring these policies, see the Exchange product documentation.
- If you do not use Microsoft Exchange integration for all users in your deployment, you need to add Skype for Business Server archiving databases (SQL Server databases) to your topology, publish the updated topology, and then configure archiving policies and settings for your users. You can deploy archiving databases at the same time that you deploy your initial topology or after you have deployed at least one Front End pool or Standard Edition Server. This document describes how to deploy archiving databases by adding them to an existing deployment.

If you enable archiving on one Front End pool or Standard Edition Server, you should enable it for all other Front End pools and Standard Edition Servers in your deployment. This is because users whose communications are required to be archived can be invited to a group IM conversation or meetings hosted on a different pool. If archiving is not enabled on the pool where the conversation or meeting is hosted, the complete session may not be archived. In these cases, IMs with archiving-enabled users still can be archived, but not for conferencing content files, and conference join or leave events.

### IMPORTANT

If archiving is critical in your organization for compliance reasons, be sure to deploy archiving, configure policies and other options at the appropriate level, and then turn on archiving for all appropriate users, before you enable those users for Skype for Business Server.

The following table provides an overview of the steps required to deploy archiving in an existing topology.

PHASE	STEPS	ROLES AND GROUP MEMBERSHIPS	DOCUMENTATION
-------	-------	-----------------------------	---------------

PHASE	STEPS	ROLES AND GROUP MEMBERSHIPS	DOCUMENTATION
<p><b>Install prerequisite hardware and software</b></p>	<p>To use Microsoft Exchange integration (using Exchange for archiving storage for some or all users), you need an existing Exchange deployment.</p> <p>To use separate archiving databases (using SQL Server databases) for archiving storage for some or all users, SQL Server on the server that will store archiving data.</p> <p>Archiving runs on Front End Servers of an Enterprise pool and Standard Edition Servers. It has no additional hardware or software requirements beyond what is required to install those servers.</p>	<p>Domain user who is a member of the local administrators group.</p>	<p><a href="#">Server requirements for Skype for Business Server 2015</a></p> <p><a href="#">Environmental requirements for Skype for Business Server 2015</a></p> <p><a href="#">Plan to integrate Skype for Business and Exchange System requirements for Skype for Business Server 2019</a></p>
<p><b>Create the appropriate internal topology to support archiving (only if not using Microsoft Exchange integration for all users in your deployment)</b></p>	<p>Run Topology Builder to add Skype for Business Server archiving databases (SQL Server databases) to the topology, and then publish the topology.</p>	<p>To define a topology to incorporate archiving databases, an account that is a member of the local users group.</p> <p>To publish the topology, an account that is a member of the domain admins group and RTCUniversalServerAdmins group, and that has full control permissions (read/write/modify) on the file share to be used for the Skype for Business Server file store (so that Topology Builder can configure the required DACLs).</p>	<p><a href="#">Add archiving databases to an existing deployment in Skype for Business Server</a></p>
<p><b>Configure server-to-server authentication (only if using Microsoft Exchange integration)</b></p>	<p>Configure servers to enable authentication between Skype for Business Server and Exchange. We recommend running <b>Test-CsExchangeStorageConnectivity testuser_sipUri - Folder Dumpster</b> to validate Exchange archiving storage connectivity before enabling archiving.</p>	<p>An account with the appropriate permissions for managing certificates on the servers.</p>	<p>Manage server-to-server authentication</p>

PHASE	STEPS	ROLES AND GROUP MEMBERSHIPS	DOCUMENTATION
<p><b>Configure archiving options and policies</b></p>	<p>Configure archiving, including whether to use Microsoft Exchange integration, the global policy and any site and user policies (when not using Microsoft Exchange integration for all data storage), and specific archiving options, such as critical mode and data export and purging. If using Microsoft Exchange integration, configure Exchange In-Place Hold policies as appropriate.</p>	<p>RTCUniversalServerAdmins group (Windows PowerShell only) or assign users to the CSArchivingAdministrator or CSAdministrator role.</p>	<p><a href="#">Configure archiving options for Skype for Business Server</a> Exchange product documentation (if using Microsoft Exchange integration).</p>

# Add archiving databases to an existing deployment in Skype for Business Server

8/7/2019 • 5 minutes to read

**Summary:** Read this topic to learn how to add archiving databases to your Skype for Business Server deployment.

You must incorporate archiving into your topology before you can configure your deployment to support archiving. The information in this topic explains how to use Topology Builder to:

- Add an archiving database to your topology.
- Publish the updated topology to add the archiving database to your Skype for Business Server deployment.

## NOTE

If you want to use Microsoft Exchange integration to store archiving data and files on Exchange servers for all your users in your deployment, do not specify **Archiving SQL Server store** or **Use SQL Server Store mirroring** information.

## Add an archiving database to your topology

1. On a computer that is running Skype for Business Server, or on which the Skype for Business Server administrative tools are installed, log on by using an account that is a member of the local Users group (or an account with equivalent user rights).
2. Start Topology Builder.
3. In the console tree, navigate to the Front End pool in which you want to deploy Archiving, and then click the name of the Front End pool where you want to deploy archiving.
4. In the **Action** menu, click **Edit Properties**.
5. In the **Edit Properties** dialog box, click **General**.
6. Scroll down to **Archiving**.
7. Select the **Archiving** check box.
8. Under **Archiving SQL Server store**, do one of the following:
  - To use an existing SQL Server store, in the drop-down list box, click the name of the SQL Server store that you want to use. If all of your users are homed on Microsoft Exchange Server 2013 or above, you can archive Skype for Business communications for all your users in Exchange. In this case, you don't need to configure SQL Server Archiving store.
  - To specify a new SQL Server store, click **New**, and then in the **Define New SQL Server Store** dialog box, do the following:
    - In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server store.
    - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named instance**, and then specify the instance you want to use.
    - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in**

**mirroring relation** check box, and then, in **Mirror port number**, specify the port number.

9. If you want to use SQL Server store mirroring, select **Enable SQL Server Store mirroring**, and then do the following:
  - To use an existing SQL Server store for mirroring, in the **Archiving SQL Server store mirror** drop-down list box, click the name of the SQL Server store that you want to use for mirroring.
  - To specify a new SQL Server store for mirroring, click **New**, and then in the **Define New SQL Server Store** dialog box, do one of the following:
    - a. In **SQL Server FQDN**, specify the FQDN of the SQL Server on which you want to create the new SQL Server store.
    - b. Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use.
    - c. If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
  - If you enable SQL Server mirroring and want to include a SQL Server mirroring witness (a third, separate SQL Server instance that can detect the health of the primary SQL Server and mirror instances), select the **Use SQL Server mirroring witness to enable automatic failover** check box, and then do one of the following:
    - a. In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server mirroring witness.
    - b. Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use for the mirroring witness.
    - c. If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
10. To save the configuration, click **OK**.

### **Publish the updated topology to add an archiving database to your deployment**

1. On a computer that is running Skype for Business Server, or on which the Skype for Business Server administrative tools are installed, log on using an account that is a member of the local Users group (or an account with equivalent user rights).

#### **NOTE**

You can define a topology by using an account that is a member of the local Users group, but to publish a topology, which is required to add a server to the topology, you must use an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (read, write, and modify) on the file share that you are using for the Skype for Business Server file store (so that Topology Builder can configure the required discretionary access control list (DACLS), or an account with equivalent rights).

2. Open the topology you created in the previous section using Topology Builder.
3. In the console tree, right-click **Skype for Business Server**, and then click **Publish Topology**.
4. On the **Publish the topology** page, click **Next**.
5. On the **Create databases** page, verify that the database is selected, and then click **Next**.

**NOTE**

If you do not have the appropriate permissions to create databases, you can cancel the selection of the database and someone with appropriate permissions can create the database. > Only databases on dedicated SQL Servers can be installed by using Topology Builder. Databases on SQL Servers that are collocated with other server components must be installed by running local setup on that computer.

6. On the **Publishing wizard complete** page, verify that the topology was successfully published, and then click **Finish**.

**IMPORTANT**

After publishing the topology, you must configure options and policies for Archiving before any content can be archived. For details, see [Configure archiving options for Skype for Business Server](#) and [Configure archiving policies for Skype for Business Server](#).

# Configure archiving options for Skype for Business Server

8/7/2019 • 5 minutes to read

**Summary:** Read this topic to learn how to configure initial archiving options for Skype for Business Server. You initially set up archiving configurations when you deploy archiving, but you can change, add, and delete configurations after deployment.

To configure initial archiving configurations, you use Skype for Business Server Control Panel to specify the following:

- Global-level configuration that is created by default when you deploy Skype for Business Server
- Optional site-level configurations that specify how archiving is implemented for a specific site
- Optional pool-level configurations that specify how archiving is implemented for a specific pool

You will need to configure options for the following:

- Whether to enable or disable archiving
- Whether to archive IM sessions
- Whether to archive web conferencing sessions
- Whether to block activity when archiving is not available
- Whether to use Exchange integration
- How to set up purging and exporting of data

## NOTE

You should specify all appropriate options before enabling archiving.

For details about how archiving configurations are implemented, including which options you can specify and the hierarchy of archiving configurations, see [Plan for archiving in Skype for Business Server](#). For details about how to manage configurations after deployment by using the Control Panel or by using Windows PowerShell, see [Manage archiving options in Skype for Business Server](#).

## Configure global level archiving options

When you add archiving to your topology and publish the topology, Skype for Business Server creates a global configuration for archiving. By default, no archiving options are enabled in the global configuration. The global configuration controls which options are enabled for your entire deployment, unless you set up site or pool configurations, which override the global configuration.

To configure archiving options at the global level:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.

3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Archiving Setting - Global**, in the **Archiving setting** drop-down list, select one of the following archiving options:
  - **Disable archiving**
  - **Archive IM sessions**
  - **Archive IM and web conferencing sessions**
6. Also on the **Edit Archiving Setting - Global** page, do the following:
  - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
  - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
  - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
    - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
    - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
7. Click **Commit**.

## Configure site level archiving options

You can specify archiving options for a specific site. A site configuration overrides the global configuration, but only for the site specified in the site configuration.

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **New**, and then click **Site Configuration**.
5. In **Select a Site**, select the site to be configured for archiving.
6. In **New Archiving Setting**, in the **Archiving setting** drop-down list box, do one of the following:
  - To enable archiving only for instant messaging (IM) sessions, click **Archive IM sessions**.
  - To enable archiving for both IM sessions and conferences, click **Archive IM and web conferencing sessions**.
  - To disable archiving for the policy, click **Disable archiving**.
7. Also in **New Archiving Setting**, do the following:
  - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.



- To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
- To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
  - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
  - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.

8. Click **Commit**.

## Configure pool level archiving options

You can specify archiving options for a specific pool. A pool configuration overrides the global configuration and site configuration, but only for the pool specified in the pool configuration.

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **New**, and then click **Pool Configuration**.
5. In **Select a Service**, select the pool to be configured for archiving.
6. In **New Archiving Setting**, in the **Archiving setting** drop-down list, select one of the following archiving options:
  - **Disable archiving**
  - **Archive IM sessions**
  - **Archive IM and web conferencing sessions**
7. Also in **New Archiving Setting** page, do the following:
  - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
  - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
  - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
    - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
    - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
8. Click **Commit**.

# Configure archiving policies for Skype for Business Server

8/7/2019 • 6 minutes to read

**Summary:** Read this topic to learn how to configure initial archiving policies for Skype for Business Server users.

In Skype for Business Server, you use policies to enable and disable archiving for internal communications and external communications for users who are homed on Skype for Business Server. This includes the following:

- A global policy that is created by default when you deploy Skype for Business Server
- Optional site-level policies that specify how archiving is implemented for a specific site
- Optional user-level policies that specify how archiving is implemented for specific users

You initially set up archiving policies when you deploy archiving, but you can change, add, and delete policies after deployment. In Skype for Business Server Control Panel, you can use the **Archiving Policy** page of the **Archiving and Monitoring** group to manage policies at the global, site, and user levels.

## NOTE

To control the implementation of archiving, you must specify options, such as whether to archive IM or conferencing, the use of critical mode, and purging options. By default no options are enabled in the global archiving configuration or any site or pool archiving configuration. You should specify all appropriate options before enabling archiving for internal or external communications. For details, see [Configure archiving options for Skype for Business Server](#).

## NOTE

If you enable Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange and have their mailboxes put on In-Place Hold.

For details about how archiving policies work, including the hierarchy for global, site, and user policies, see [Plan for archiving in Skype for Business Server](#). For details about how to manage policies after deployment, see [Manage archiving policies in Skype for Business Server](#).

## Global policy

When you deploy your Front End Servers, Skype for Business Server creates a global policy for archiving. By default, archiving is disabled in the global policy. The global policy controls whether archiving is enabled for internal and external communications for your entire deployment, unless you set up site or user policies, which override the global policy, or if you use Microsoft Exchange integration for some or all of your users. If you use Microsoft Exchange integration, the global policy does not apply to any users who are homed on Exchange and have the mailboxes put on In-Place Hold.

### Configure the global policy for archiving for Skype for Business Server archiving databases

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.

3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. On the **Archiving Policy** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Archiving Policy - Global**, do the following:
  - In **Name**, if you do not want to use the default name of Global, specify a new name for the global policy.
  - In **Description**, provide information about what the policy is (for example, Global policy for *divisionName*).
  - To control archiving of internal communications for all sites and users not specifically controlled through a site policy or user policy, select or clear the **Archive internal communications** check box.
  - To control archiving of external communications for all sites and users not specifically controlled through a site policy or user policy, select or clear the **Archive external communications** check box.
6. Click **Commit**.

## Site policies

You can enable or disable archiving for specific sites by creating an archiving policy for each of those sites. A site policy overrides the global policy, but user policies override site policies. Archiving policies only apply if you do not use Microsoft Exchange integration or, if you do use Microsoft Exchange integration, but have some users who are not homed on Exchange and have their mailboxes put on In-Place Hold.

### Create an archiving policy for a site

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.

For details about how archiving policies work, including the hierarchy for global, site, and user policies, see [Plan for archiving in Skype for Business Server](#).

4. Click **New**, and then click **Site policy**.
5. In **Select a site**, click the site to which the policy is to be applied.
6. In **New Archiving Policy**, do the following:
  - In **Name**, specify the name for the site policy.
  - In **Description**, provide information about what the site policy is (for example, site policy for Redmond).
  - To control archiving of internal communications for the specified site, select or clear the **Archive internal communications** check box.
  - To control archiving of external communications for the specified site, select or clear the **Archive external communications** check box.
7. Click **Commit**.

## User policies

You can enable or disable archiving for specific users by creating and configuring an archiving policy for users, and then applying the policy to specific users or user groups. User policies override any global policy or site policies. Archiving policies only apply if you do not use Microsoft Exchange integration or, if you do use Microsoft Exchange integration, but have some users who are not homed on Exchange and have their mailboxes put on In-Place Hold.

### Configure an archiving policy for users homed on Skype for Business Server

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. Click **New**, and then click **User policy**.
5. In **New Archiving Policy**, do the following:
  - In **Name**, specify the name for the user policy.
  - In **Description**, provide information about what the user policy is (for example, user policy for legal department).
  - To control archiving of internal communications for the user policy, select or clear the **Archive internal communications** check box.
  - To control archiving of external communications for the user policy, select or clear the **Archive external communications** check box.
6. Click **Commit**.

A user policy applies only to users to whom you assign the policy.

### Apply a Skype for Business Server archiving policy to a user

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**, and then search for the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Skype for Business Server user** under **Archiving policy**, select the archiving user policy that you want to apply.

#### NOTE

The <**Automatic**> settings apply the default server installation settings. These settings are applied automatically by the server.

6. Click **Commit**.

# Configure archiving disclaimers for external users in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Read this topic to learn how to configure an archiving disclaimer for Skype for Business Server.

If your organization communicates with external partners, you need to let them know that you are archiving communications with them. When you deploy an Edge Server and enable federation for your organization, you are asked whether you want to automatically send an archiving disclaimer to external partners.

If you need to change this configuration, you can use the Skype for Business Server Control Panel or the Windows PowerShell **Set-CsAccessEdgeConfiguration** cmdlet. Cmdlets can be run either from the Skype for Business Server management shell or from a remote session of Windows PowerShell.

To enable external users to collaborate with users in your Skype for Business Server deployment, you must also configure at least one external access policy to support external user access. For details, see [Manage XMPP Federated Partners for Your Organization](#). For details about controlling access for specific federated domains, see [Control Access by Individual Federated Domains](#).

## Enable or disable archiving disclaimer using the Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Federation and External Access**, and then click **Access Edge Configuration**.
4. On the **Access Edge Configuration** tab, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, under **Enable federation and public IM connectivity**, select or clear the **Send archiving disclaimer to federated partners** check box to enable or disable automatically sending the archiving disclaimer.
6. Click **Commit**.

## Enable or disable archiving disclaimer using Windows PowerShell

To enable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to True (\$True):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $True
```

To disable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to False (\$False):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $False
```

# Configure integration with Exchange storage for Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Read this topic to learn how to configure integration with Exchange storage in Skype for Business Server.

If you use Microsoft Exchange integration for all users in your deployment, you don't need to configure Skype for Business Server archiving policies for your users. Instead, you configure Exchange In-Place Hold policies to support archiving for users homed on Exchange, with their mailboxes put on In-Place Hold. Before you configure integration with Exchange storage, read [Plan for archiving in Skype for Business Server](#). For details about Exchange In-Place Hold policies, see the Exchange product documentation.

## Configure integration with Microsoft Exchange storage

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Click the name of the appropriate global, site, or pool configuration in the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
  - To enable integration with Exchange storage, select the **Microsoft Exchange integration** check box.
  - To disable integration with Exchange storage, clear the **Microsoft Exchange integration** check box.
5. Click **Commit**.

## When Skype for Business Server and Microsoft Exchange are deployed in different forests

If you use Microsoft Exchange integration and Microsoft Exchange Server is not deployed in the same forest as Skype for Business Server, you must make sure that the following Exchange Active Directory attributes are synchronized to the forest where Skype for Business Server is deployed:

- msExchUserHoldPolicies
- proxyAddresses

This is a multi-value attribute. When synchronizing this attribute, you need to merge the values, not replace them to ensure the existing values are not lost.

# Deploy monitoring in Skype for Business Server

8/7/2019 • 6 minutes to read

**Summary:** Learn how to deploy monitoring in Skype for Business Server.

Before performing these tasks, review [Plan for monitoring in Skype for Business Server](#).

You will typically implement monitoring services within your topology by completing the following two steps:

1. Enabling monitoring at the same time you set up a new Skype for Business Server pool. (In Skype for Business Server, monitoring is enabled or disabled on a pool-by-pool basis.) Note that you can enable monitoring for a pool without actually collecting monitoring data, a process explained in the Configuring Call Detail Recording and Quality of Experience Settings section of this documentation.
2. Associating a monitoring store (that is, a monitoring database) with the new pool. Note that a single monitoring store can be associated with multiple pools. Depending on the number of users homed on your Registrar pools, that means that you do not have to set up a separate monitoring database for each of your pools. Instead, single monitoring store can be used by multiple pools.

Although it's often easier to enable monitoring at the same time that you create a new pool, it's also possible to create a new pool with monitoring disabled. If you do that, you can later use Topology Builder to enable the service: Topology Builder provides a way to enable or disable monitoring for a pool, or to associate a pool with a different monitoring store. Keep in mind that even though there is no longer a Monitoring Server role you will still need to create one or more monitoring stores: back-end databases used to store the data gathered by the monitoring service. These back-end databases can be created using Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, or Microsoft SQL Server 2014.

## NOTE

If monitoring has been enabled for a pool you can disable the process of collecting monitoring data without having to change your topology: Skype for Business Server provides a way for you to disable (and then later re-enable) Call Detail Recording (CDR) or Quality of Experience (QoE) data collection. For more information, see the Configuring Call Detail Recording and Quality of Experience Settings section of this document.

One other important enhancement to monitoring in Skype for Business Server is the fact that Skype for Business Server Monitoring Reports now support IPv6: reports that use the IP Address field will display either IPv4 or IPv6 addresses depending on : 1) the SQL query being used; and, 2) where or not the IPv6 address is stored in the monitoring database.

## NOTE

Ensure that the SQL Server Agent Service Startup Type is Automatic and the SQL Server Agent Service is running for the SQL Instance which is holding the Monitoring databases, so that the Default Monitoring SQL Server Maintenance Jobs can run on their scheduled basis under the control of the SQL Server Agent Service.

This documentation walks you through the process of installing and configuring monitoring and Monitoring Reports for Skype for Business Server. The documentation provides step-by-step instructions that will help you to:

- Enable monitoring in your topology and associate a monitoring store with a Front End pool.
- Install SQL Server Reporting Services and the Skype for Business Server Monitoring Reports. Monitoring

Reports are preconfigured reports that provide different views into the information stored in a monitoring database.

- Configure Call Detail Recording (CDR) and Quality of Experience (QoE) data collection. Call detail recording provides a way for you to track usage of Skype for Business Server capabilities such as Voice over IP (VoIP) phone calls; instant messaging (IM); file transfers; audio/video (A/V) conferencing; and application sharing sessions. QoE metrics track the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay).
- Manually purge CDR and/or QoE records from the monitoring database.

## Deployment checklist for monitoring

Although monitoring is already installed and activated on each Front End server, there are still several steps that you must undertake before you can actually begin to collect monitoring data for Skype for Business Server. These steps are outlined in the following checklist:

PHASE	STEPS	ROLE AND GROUP MEMBERSHIP	DOCUMENTATION
<b>Install prerequisite hardware and software</b>	Install a supported version of Microsoft SQL Server on the computer that will act as the backend data store for monitoring.	Domain user who is also a member of the local administrators group.	<a href="#">Supported Hardware Server Software and Infrastructure Support</a>
<b>Create the appropriate internal topology to support monitoring</b>	Use Skype for Business Server Topology Builder to add monitoring databases to the topology, then published the updated topology.	To define a topology, a user who is a member of the local users group. To publish the topology, a user who is a member of the domain administrators group and the RTCUniversalServerAdmins group.	<a href="#">Associate a monitoring store with a Front End pool in Skype for Business Server</a>
<b>Enable the appropriate monitoring settings</b>	Enable Call Detail Recording (CDR) and/or Quality of Experience (QoE) monitoring at the global and/or the site scopes.	A user who is a member of the RTCUniversalServerAdmins group or who has been assigned an RBAC role that provides access to the CsCdrConfiguration and CsQoEConfiguration cmdlets.	<a href="#">Configure call detail recording and Quality of Experience settings in Skype for Business Server</a>

## Enable monitoring

Although the unified data collection agents are automatically installed and activated on each Front End server, that does not mean that you will automatically begin to collect monitoring data the moment you finish installing Skype for Business Server. Instead, you must do two things: you must associate your Front End servers/Front End pools with a monitoring database, and you must enable Call Detail Recording (CDR) and/or Quality of Experience (QoE) monitoring at the global scope and/or the site scope.

For step-by-step instructions on associating Front End servers or Front End pools with a monitoring database, see the topic [Associate a monitoring store with a Front End pool in Skype for Business Server](#) in the Deployment guide. After these associations have been made, and after your new Skype for Business Server topology has been



published, you will still not be able to collect monitoring data. That's because, by default, both CDR and QoE data collection is disabled when you install Skype for Business Server.

In order to begin data collection you will need to enable CDR and/or QoE monitoring. (Note that you do not have to enable both CDR and QoE monitoring; if you prefer, you can enable one type of monitoring while leaving the other type disabled.) To enable CDR monitoring at the global scope run the following command from within the Skype for Business Server Management Shell:

```
Set-CsCdrConfiguration -Identity "global" -EnableCDR $True
```

Alternatively, you can enable CDR monitoring from within the Skype for Business Server Control Panel. From within the Skype for Business Server Control Panel, complete the following procedure:

1. Click **Monitoring**.
2. On the **Call Detail Recording** tab, double-click the **Global** setting.
3. In the **Edit Call Detail Recording (CDR) Setting** pane, select **Enable monitoring of CDRs** and then click **Commit**.

To enable QoE monitoring at the global scope, run this command from within the Skype for Business Server Management Shell:

```
Set-CsQoEConfiguration -Identity "global" -EnableQoE $True
```

If you prefer, you can also enable QoE monitoring from within the Skype for Business Server Control Panel. From within the Control Panel, complete the following procedure:

1. Click **Monitoring**.
2. On the **Quality of Experience Data** tab, double-click the **Global** setting.
3. In the **Edit Quality of Experience (QoE) Setting** pane, select **Enable monitoring of QoE data** and then click **Commit**.

As noted, the preceding examples enable monitoring at the global scope; that is, they enable CDR and QoE monitoring throughout your organization. Alternatively, you can create separate CDR and QoE configuration settings at the site scope, and then selectively enable or disable monitoring for each site. For example, you could enable CDR monitoring for your Redmond site, yet disable CDR monitoring for your Dublin site. For more information on managing your monitoring configuration settings, see the Deployment guide topic [Configure call detail recording and Quality of Experience settings in Skype for Business Server](#).

## See also

[Plan for monitoring in Skype for Business Server](#)

# Associate a monitoring store with a Front End pool in Skype for Business Server

8/7/2019 • 4 minutes to read

**Summary:** Learn how to associate Front End pools with a monitoring store used by Skype for Business Server.

In Skype for Business Server, monitoring data can only be collected on Front End pools that have been associated with a monitoring store, a task typically carried out when you define a Front End pool in Topology Builder.

## Associate a monitoring store with a Front End pool

To associate a monitoring store with a new Front End pool, make sure that you select the option **Monitoring (call detail recording and logging of quality of experience metrics)** on the **Select Features** page of the Define New Front End Pool wizard. Note that, if you select this option, you must also specify a SQL store in order to complete the wizard; however, this store does not have to exist at the time you run the wizard. That means that you can first associate a pool with a monitoring store, then later setup and configure that store.

Alternatively, you can associate an existing Front End pool with a new or different monitoring store by completing the following procedure:

1. Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server Topology Builder**.
2. In the **Topology Builder** dialog box, select **Download Topology from existing deployment** and then click **OK**.
3. In the **Save As** dialog box, enter a file name for your current topology and then click **Save**. The saved topology can later be retrieved and re-published in case there are problems with the new topology.
4. In Topology Builder, expand **Skype for Business Server**, expand the name of the site containing the Front End pool, then click expand **Enterprise Edition Front End pools**.
5. Right-click the name of the pool to be associated with the monitoring store and then click **Edit Properties**.
6. In the **Edit Properties** dialog box, on the **General** tab, select the option **Monitoring (CDR and QoE metrics)** and then select an existing SQL Server database from the **Monitoring SQL Server store** dropdown list. (Or, click **New** to associate the pool with a new database store.) If you choose to use a new database store then, in the **Define New SQL Store** dialog box, enter the fully qualified domain name of the SQL Server computer in the **Sql Server FQDN** box. If you want to use the default SQL Server instance for that store select **Default Instance**; otherwise select **Named Instance** and enter the instance name in the **Named Instance** box.

The **Edit Properties** dialog box also gives you the option of creating a SQL mirror for your monitoring database (a SQL mirror enables you to maintain two copies of your monitoring database, one copy stored on the monitoring store computer and the other on the SQL mirror computer). To enable mirroring, select **This SQL instance is in mirroring relation** and enter the port number for the mirror server in the **Mirroring port number** box.

7. In the **Edit Properties** dialog box, click **OK**.

After associating the monitoring store with a Front End pool you must publish the new topology before the changes take effect. To publish your new topology, complete the following steps in Topology Builder:

1. Click **Action**, point to **Topology**, and then click **Publish**.
2. In the Publish Topology wizard, on the **Publish the topology** page, click **Next**.
3. On the **Publishing wizard complete** page, click **Finish**.

After the topology has been published you can then install the monitoring database on the computer that will host the monitoring store. The monitoring database can be installed by using the Skype for Business Server Management Shell and Windows PowerShell. To install the database locally (that is, to install the database on the same computer where you are running the Skype for Business Server Management Shell), start the Management Shell on the appropriate computer, then type in the following command and press ENTER:

```
Install-CsDatabase -LocalDatabases
```

When you run the preceding command, Install-CsDatabase will read the current Skype for Business Server topology, determine which databases need to be installed on the local computer, and then automatically install and configure each of those databases.

To install the database on a remote computer (that is, a computer other than the computer where the Management Shell is running) you must include at least two parameters: the ConfiguredDatabases parameter and the SqlServerFqdn parameter. These parameters tell the Install-CsDatabase cmdlet to retrieve the Skype for Business Server topology and then install and configure the required databases on the computer specified by the SqlServerFqdn parameter. The SqlServerFqdn parameter must use a parameter value representing the fully qualified domain name of the computer where the databases are to be installed.

For example, this command installs the monitoring database on the computer atl-sql-001.litwareinc.com:

```
Install-CsDatabase -ConfiguredDatabases -SqlServerFqdn atl-sql-001.litwareinc.com
```

Alternatively, you can install the monitoring database by running the Skype for Business Server Deployment Wizard on the computer that will host the monitoring store. To do this, log on to the appropriate computer and complete the following procedure:

1. Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server Deployment Wizard**.
2. In the Deployment Wizard, click **Install or Update Skype for Business Server System**.
3. On the **Deploy** page, under **Step 2: Setup or Remove Skype for Business Server Components**, click **Run Again**.
4. In the Setup Skype for Business Server components wizard, on the **Setup Skype for Business Server components** page, click **Next**.
5. On the **Specify path to MSIs** page, type the path to the file Ocscore.msi (a file included with your Skype for Business Server installation media) and then click **Next**.
6. On the **Executing Commands** page, click **Finish**.

To ensure that all the required Skype for Business Server services have started, click **Run** under the heading **Step 4: Start Services** on the **Deploy** page

# Install SQL Server Reporting Services in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn where to go to find information about SQL Server Reporting Services used by Skype for Business Server.

Skype for Business Server can use SQL Server Reporting Services (SSRS) for viewing and monitoring reports. In order to use this functionality you will need to have Reporting Services installed and configured.

## Install SQL Server Reporting Services

If you intend to use Skype for Business Server Monitoring Reports (see the next article of this documentation for more information) you must first install SQL Server Reporting Services; Reporting Services can be installed at the same time you install Microsoft SQL Server or any time after SQL Server has been installed. If you have not installed SQL Server, then follow the instructions provided earlier in this documentation. When installing SQL Server, make sure that, on the Feature Selection page, you select Reporting Services. That will install SQL Server Reporting Services.

To learn how to install SQL Server Reporting Services, see [SQL Server Reporting Services \(SSRS\)](#).

If you have already installed SQL Server but did not install SQL Server Reporting Services you can add that feature by following the appropriate set of instructions for SQL Server Reporting Services.

# Install Monitoring Reports in Skype for Business Server

8/7/2019 • 6 minutes to read

**Summary:** Learn how to install a service that will generate Monitoring reports in Skype for Business Server.

Skype for Business Server Monitoring Reports provide you with a wealth of information about the quality and quantity of the communication sessions that take place in your organization.

## Install Monitoring Reports

Monitoring Reports are not automatically installed when you install Skype for Business Server; instead, you must install Monitoring Reports separately, and only after Skype for Business Server has been installed on the computer.

### NOTE

It is recommended that you install Monitoring Reports on the same computer where the monitoring database is installed. This simplifies the process of assigning permissions for accessing the reports: installing Monitoring Reports on the computer that hosts the monitoring store means that you will not have to configure permissions that allow a database on one computer to interact with Reporting Services running on a second computer.

Skype for Business Server Monitoring Reports include over 30 reports designed to provide detailed information about conferences, peer-to-peer IM sessions, user registrations, the Response Group application, and much more. For the 2013 version, Skype for Business Server Monitoring Reports include a number of enhancements:

- **New voice quality reports.** These new reports include the [Media Quality Comparison Report in Skype for Business Server](#), which compares quality between different types of calls (for example, between wired calls and wireless calls); and the [Conference Join Time Report in Skype for Business Server](#), which provides information regarding the amount of time requires for users to join a conference.
- **Improved reports for analyzing and troubleshooting both video and application sharing sessions.** the [Media Quality Summary Report in Skype for Business Server](#) provides a way to analyze video and application sharing calls, while the [Server Performance Report in Skype for Business Server](#) details the performance of servers generating these calls. Video and application sharing metrics are also now reported by the [Peer-to-Peer Session Detail Report in Skype for Business Server](#) and the [Conference Detail Report in Skype for Business Server](#).
- **Improved report performance.** This includes faster response and data retrieval time, as well as faster and easier navigation through the reports.

More information on the individual reports can be found in the Monitoring Reports documentation.

### NOTE

There is another report - QoE Call Detail Subreport - included in Skype for Business Server. However, this report is primarily for internal use, and is not intended to be directly accessed.

There are two ways to install Skype for Business Server Monitoring Reports: you can use the Skype for Business Server Deployment Wizard or you can use a Windows PowerShell script included with the Skype for Business Server installation files. Regardless of the method you use to install the reports you must first make sure that you:

- Have the right to add a database role to a user account in the monitoring database.
- Hold the Content Manager role in SQL Server Reporting Services. This role gives you the right to deploy reports to SQL Server Reporting Services.

To install the Monitoring Reports by using the Deployment Wizard, complete the following steps:

1. Click **Start**, click **All Programs**, click **Skype for Business Server**, and then click **Skype for Business Server Deployment Wizard**.
2. In the Deployment Wizard, click **Deploy Monitoring Reports** in order to start the Deploy Monitoring Reports wizard.
3. In the Deploy Monitoring Reports wizard, on the **Specify Monitoring Database** page, make sure that the fully qualified domain name of the computer hosting your monitoring store appears in the **Monitoring database** dropdown list. (If you have multiple monitoring stores you will need to select the appropriate server from the dropdown list.) Verify that the correct SQL Server instance appears in the **SQL Server Reporting Services (SSRS) instance** box (for example, **atl-sql-001.litwareinc.com/archinst**) and then click **Next**.
4. On the **Specify Credentials** page, in the **User name** box, type the domain name and user name of the account to be used when accessing the Monitoring Reports (for example, **litwareinc\kenmyer**). If you do not use this format (domain\user name) an error will occur.

Type the user account password in the **Password** box, and then click **Next**. Note that no special rights are required for this account. The account will automatically be granted the required logon and database permissions when setup completes.

5. On the **Specify Read-Only Group** page enter the name of a security group that will be granted read-only access to the SQL Server Reporting Services in the User group box. For example, to give read-only administrators access to the reports enter **RTCUniversalReadOnlyAdmins**. Click **Next**.
6. On the **Executing Commands** page, click **Finish**.

Monitoring Reports can also be installed from the Skype for Business Server Management Shell by running the script `DeployReports.ps1`; this Windows PowerShell script can be found in the `<install location>\Skype for Business Server 2015\Deployment\Setup` folder. To install Monitoring Reports using `DeployReports.ps1`, type a command similar to the following at the Management Shell prompt:

```
C:\Program Files\Skype for Business Server 2015\Deployment\Setup\DeployReports.ps1 -storedUserName
"litwareinc\kenmyer" -storedPassword "p@ssw0rd" -readOnlyGroupName "RTCUniversalReadOnlyAdmins" -
reportServerSqlInstance "atl-sql-001.litwareinc.com" -monitoringDatabaseId "MonitoringDatabase:atl-sql-
001.litwareinc.com"
```

The parameters used in the preceding command are described in the following table:

PARAMETER NAME	REQUIRED	DESCRIPTION
storedUserName	Yes	User account (in the format domain\username) used to access the monitoring store; for example: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">           -storedUserName            "litwareinc\kenmyer"         </div> This account must have the previously-specified SQL Server and SQL Server Reporting Services permissions or the script will fail.

PARAMETER NAME	REQUIRED	DESCRIPTION
storedPassword	Yes	Password for the user account used to access the monitoring store.
readOnlyGroupName	No	Domain or local security group whose members will be granted read-only access to the Monitoring Reports. Note that the script will fail if the specified group does not exist. If you later decide to revoke these permissions, or if you decide to grant other users or other groups access permissions, you can do so using the SQL Service Reporting Services Report Manager.
reportSqlServerInstance	No	SQL Server instance that hosts the Reporting Service. The Reporting instance must be specified using the fully qualified domain name of the Report Server; for example: <pre>-reportServerSqlInstance atl-sql-001.litwareinc.com</pre> If this parameter is not included the script will assume that the reporting services are hosted by the same SQL Server instance that hosts the monitoring database.
monitoringDatabaseId	No	Service Identity for the monitoring database. You can return the Identities for your monitoring databases by running this command: <pre>Get-CsService -MonitoringDatabase</pre>

After the Monitoring Reports have been installed you must then use the `New-CsReportingConfiguration` cmdlet to configure the URL used to access these reports. This task can be carried out from the Skype for Business Server Management Shell by running the following Windows PowerShell command. Note that it is recommended, but not required, that you use the HTTPS protocol when configuring the reporting URL:

```
New-CsReportingConfiguration -Identity 'service:MonitoringDatabase:atl-sql-001.litwareinc.com' -ReportingURL 'https://atl-sql-001.litwareinc.com:443/Reports_ARCHINST'
```

In the preceding command, the `ReportingUrl` property should be set to the Report Manager URL used by SQL Server 2008 R2 Reporting Services. You can determine the Report Manager URL by completing the following steps on the computer where SQL Server Reporting Services has been installed:

1. Click Start, click All Programs, click Microsoft SQL Server 2008 R2, click Configuration Tools, and then click Reporting Services Configuration Manager.
2. In the Reporting Services Configuration Connection dialog box, make sure that the name of the Reporting Services computer appears in the Server Name box. Select the SQL Server instance from the Report Server Instance dropdown list and then click Connect.
3. In Reporting Services Configuration Manager, click Report Manager URL. One or more URLs should appear in the Report Manager URL pane. Any of these URLs can be used as the Reporting URL although, again, it is recommended that the `ReportingUrl` use the HTTPS protocol.

If you have set up a mirror database for your monitoring database then you must also associate the Monitoring Reports with the mirror database. See the article [Associate Monitoring Reports with a mirror database in Skype for Business Server](#) for details.



# Associate Monitoring Reports with a mirror database in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to associate Monitoring Reports with a mirror database used by Skype for Business Server.

## Monitor reports with a mirror database

If you configure a mirror for your monitoring database, that mirror database will take over as the primary database if a failover occurs. However, if you use Skype for Business Server Monitoring Reports and a failover occurs, you might find that your Monitoring Reports are not connecting to the mirror database. This is because, when you install Monitoring Reports, you specify only the location of the primary database; you do not specify the location of the mirror database.

To get Monitoring Reports to automatically failover to the mirror database, you must add the mirror database as a "failover partner" to the two databases that are used by Monitoring Reports (one database for Call Detail Record data, and the other for Quality of Experience (QoE) data). (Note that this step should be performed after you have installed Monitoring Reports.) You can add the failover partner information by manually editing the connection string values used by these two databases. To do that, complete the following procedure:

1. Use Internet Explorer to open the **SQL Server Reporting Services** home page. The Reporting Services home page URL includes:

- The **http:** prefix.
- The fully qualified domain name (FQDN) of the computer where the Reporting Services are installed (for example, **atl-sql-001.litwareinc.com**).
- The character string **/Reports\_**.
- The name of the database instance where the Monitoring Reports are installed (for example, **archinst**).

For example, if SQL Server Reporting Services was installed on the computer atl-sql-001.litwareinc.com and the Monitoring Reports use the database instance archinst, the home page URL would look like this:

[http://atl-sql-001.litwareinc.com/Reports\\_archinst](http://atl-sql-001.litwareinc.com/Reports_archinst)

2. After you have accessed the Reporting Services home page, click **ServerReports**, and then click **Reports\_Content**. That will take you to the **Reports\_Content** page for the Skype for Business Server Monitoring Reports.

3. On the **Reports\_Content** page, click the **CDRDB** data source.

4. On the **CDRDB** page, on the **Properties** tab, look for the text box labeled **Connection string**. The current connection string will look similar to this:

```
Data source=(local)\archinst;initial catalog=LcsCDR
```

5. Edit the connection string to include the server name and database instance for the mirror database. For example, if the server is named atl-mirror-001 and the mirror database is in the archinst instance, you will need to add to specify the mirror database using this syntax:

Failover Partner=atl-mirror-001\archinst

Your edited connection string will look like this:

Data source=(local)\archinst;Failover Partner=atl-mirror-001\archinst;initial catalog=LcsCDR

6. After updating the connection string, click **Apply**.
7. On the **CDRDB** page, click the **Reports\_Content** link. Click the **QMSDB** data source, and then edit the connection string for the QoE database. For example:

Data source=(local)\archinst;Failover Partner=atl-mirror-001\archinst;initial catalog=QoEMetrics

8. Click **Apply**.

## See also

[Install Monitoring Reports in Skype for Business Server](#)

[Using Monitoring Reports in Skype for Business Server](#)

# Configure call detail recording and Quality of Experience settings in Skype for Business Server

8/7/2019 • 4 minutes to read

**Summary:** Learn how to configure CDR and QoE in Skype for Business Server.

Configure CDR and QoE monitoring using SQL Server Reporting Services reports for Skype for Business Server.

## Configure CDR and QoE

After you have associated a monitoring store with a Front End pool, set up the monitoring store, and then installed and configured SQL Server Reporting Services and Monitoring Reports you can manage Call Detail Recording (CDR) and Quality of Experience (QoE) monitoring by using Skype for Business Server Management Shell. Skype for Business Server Management Shell cmdlets allow you to enable and disable CDR and/or QoE monitoring for a particular site or for your entire Skype for Business Server deployment; that can be done with a command as simple as this:

```
Set-CsQoEConfiguration -Identity "global" -EnableQoE $False
```

When you install Skype for Business Server, you will also install a predefined collection of global configuration settings for both CDR and QoE. Default values for some of the more commonly-used settings used by Call Detail Recording are shown in the following table:

PROPERTY	DESCRIPTION	DEFAULT VALUE
EnableCDR	Indicates whether or not CDR is enabled. If True, all CDR records will be collected and written to the monitoring database.	True
EnablePurging	Indicates whether or not CDR records will periodically be deleted from the database. If True, records will be deleted after the time period specified by the properties <code>KeepCallDetailForDays</code> (for CDR records) and <code>KeepErrorReportForDays</code> (for CDR errors). If False, CDR records will be maintained indefinitely.	True
KeepCallDetailForDays	Indicates the number of days that CDR records will be kept in the database; any records older than the specified number of days will automatically be deleted. However, this will occur only if purging has been enabled. <code>KeepCallDetailForDays</code> can be set to any integer value between 1 and 2562 days (approximately 7 years).	60 days

PROPERTY	DESCRIPTION	DEFAULT VALUE
KeepErrorReportForDays	Indicates the number of days that CDR error reports are kept; any reports older than the specified number of days will automatically be deleted. CDR error reports are diagnostic reports uploaded by client applications such as Skype for Business Server. You can set this property to any integer value between 1 and 2562 days.	60 days

Similarly, default values for selected QoE settings are shown in this table:

PROPERTY	DESCRIPTION	DEFAULT VALUE
EnableQoE	Indicates whether or not QoE monitoring is enabled. If True, all QoE records will be collected and written to the monitoring database.	True
EnablePurging	Indicates whether or not QoE records will periodically be deleted from the database. If True, records will be deleted after the time period specified by the KeepQoEDataForDays property. If False, QoE records will be maintained indefinitely.	True
KeepQoEDataForDays	Indicates the number of days that QoE records will be kept in the database; any records older than the specified number of days will automatically be deleted. However, this will occur only if purging has been enabled. KeepCallDetailForDays can be set to any integer value between 1 and 2562 days.	60 days

If you need to modify these global settings you can do so by using the Set-CsCdrConfiguration and the Set-CsQoEConfiguration cmdlets. For example, this command (run from within the Skype for Business Server Management Shell) disables CDR monitoring at the global scope; that's done by setting the EnableCDR property to False (\$False):

```
Set-CsCdrConfiguration -Identity "global" -EnableCDR $False
```

Note that disabling monitoring does not dissociate the monitoring store from the Front End pool, nor does it uninstall or otherwise affect the backend monitoring database. When you use Skype for Business Server Management Shell to disable either CDR or QoE monitoring all you really do is temporarily stop Skype for Business Server from collecting and archiving monitoring data. If you want to resume, in this case, the collection and archiving of CDR data, all you need to do is set the EnableCDR property back to True (\$True):

```
Set-CsCdrConfiguration -Identity "global" -EnableCDR $True
```

Similarly, this command disables the purging of QoE records at the global scope:

```
Set-CsQoEConfiguration -Identity "global" -EnablePurging $False
```

In addition to the global settings, CDR and QoE configurations settings can be assigned to the site scope. This provides additional management flexibility when it comes to monitoring; for example, an administrator can enable CDR monitoring for the Redmond site but disable CDR monitoring for the Dublin site. To create new CDR configuration settings at the site scope, use a command similar to this:

```
New-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $False
```

Keep in mind that settings configured at the site scope take precedence over settings configured at the global scope. For example, suppose CDR monitoring is enabled at the global scope, but disabled at the site scope (for the Redmond site). That means that call detail recording information will not be archived for users in the Redmond site. However, users in other sites (that is, users managed by the global settings instead of the Redmond site settings) will have their call detail recording information archived.

New QoE configuration settings can be created at the site scope by using a command like this one:

```
New-CsQoEConfiguration -Identity "site:Redmond" -KeepQoEDataForDays 15
```

For more information, type the following commands from within the Skype for Business Server Management Shell:

```
Get-Help New-CsCdrConfiguration | more  
Get-Help Set-CsCdrConfiguration | more  
Get-Help New-CsQoEConfiguration | more  
Get-Help Set-CsQoEConfiguration | more
```

# Manually purge the call detail recording and Quality of Experience databases in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to manually purge records from the CDR and the QoE databases used by Skype for Business Server.

The CDR and QoE databases can be manually or automatically purged of records. Purging records can be important so that data doesn't become stale or when needing to reset reports from a starting baseline.

## Manually purge records from CDR and QoE databases

Administrators can configure the Call Detail Recording (CDR) and/or the Quality of Experience (QoE) databases to automatically purge old records from the database; this occurs if purging has been enabled for the specified database (CDR or QoE) and if there are any records that have been in the database longer than the specified amount of time. For example, every day at 1:00 AM administrators might configure the system so that QoE records more than 60 days old will be deleted from the QoE database.

In addition to that automatic purging, two new cmdlets — `Invoke-CsCdrDatabasePurge` and `Invoke-CsQoEDatabasePurge` — have been added to Skype for Business Server; these cmdlets allow administrators to manually purge records from the CDR and the QoE databases at any time. For example, to manually purge all the records more than 10 days old from the CDR database you can use a command similar to this:

```
Invoke-CsCdrDatabasePurge -Identity service:MonitoringDatabase:atl-sql-001.litwareinc.com -  
PurgeCallDetailDataOlderThanDays 10 -PurgeDiagnosticDataOlderThanDays 10
```

In the preceding command both call detail records and diagnostic data records older than 10 days are deleted from the monitoring database on `atl-sql-001.litwareinc.com`. (Call detail records are user/session reports. Diagnostic data records are diagnostic logs uploaded by client applications such as Skype for Business Server.)

As shown above, when you run the `Invoke-CsCdrDatabasePurge` cmdlet you must include both the `PurgeCallDetailDataOlderThanDays` and the `PurgeDiagnosticDataOlderThanDays` parameters. However, these parameters do not have to be set to the same value. For example, it's possible to purge call detail records more than 10 days old and yet, at the same time, leave all the diagnostic data records in the database. To do that, set `PurgeCallDetailDataOlderThanDays` to 10 and `PurgeDiagnosticDataOlderThanDays` to 0. For example:

```
Invoke-CsCdrDatabasePurge -Identity service:MonitoringDatabase:atl-sql-001.litwareinc.com -  
PurgeCallDetailDataOlderThanDays 10 -PurgeDiagnosticDataOlderThanDays 0
```

By default, any time you run `Invoke-CsCdrDatabasePurge` you will see a prompt similar to this one for each database table that must be purged:

```
Confirm  
Are you sure you want to perform this action?  
Performing operation "Stored procedure: RtcCleanupDiag" on Target "Target SQL Server:atl-sql-  
001.litwareinc.com\archinst Database: lcscdr".  
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

You must type either Y (for Yes) or A (for Yes to All) before the database purging will actually take place. If you

would prefer to suppress these confirmation prompts, add the following parameter to the end of your call to Invoke-CsCdrDatabasePurge:

```
-Confirm:$False
```

For example:

```
Invoke-CsCdrDatabasePurge -Identity service:MonitoringDatabase:atl-sql-001.litwareinc.com -  
PurgeCallDetailDataOlderThanDays 10 -PurgeDiagnosticDataOlderThanDays 10 -Confirm:$False
```

If you do that, confirmation prompts will not be displayed, and database purging will immediately be performed.

To purge the QoE database, use the Invoke-CsQoEDatabasePurge cmdlet and specify the age (in days) of the records to be deleted:

```
Invoke-CsQoEDatabasePurge -Identity service:MonitoringDatabase:atl-sql-001.litwareinc.com -  
PurgeQoEDataOlderThanDays 10
```

# Deploy Video Interop Server in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Deploy the VIS server role in Skype for Business Server.

Skype for Business Server can now integrate directly with Cisco teleconferencing systems (VTCs) such as the Cisco C60 or Cisco MX300. This requires the introduction of a new server role called the Video Interop Server (VIS), and correct configuration of both the VIS and the equipment it will interoperate with. A VTC registers with existing Cisco infrastructure such as Cisco Unified Communication Manager (CUCM), and a video SIP trunk is used between CUCM and the VIS pool.

## In this section

Configuring interoperability between a VIS server or pool and VTC systems requires performing the following five procedures:

- [Create a VIS pool in Skype for Business Server](#)
- [Deploy the VIS server role in Skype for Business Server](#)
- [Configure the Video Interop Server in Skype for Business Server](#)
- [Configure CUCM for Interoperation with Skype for Business Server](#)
- [Configure a VTC for Interoperation with Skype for Business Server](#)

## Related sections

[Plan for Video Interop Server in Skype for Business Server](#)



# Create a VIS pool in Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Create a Video Interop Server pool in Skype for Business Server using Topology Builder.

## Create a VIS or VIS pool using Topology Builder

1. Open Topology Builder on the front end server. From the left pane of Topology Builder, right click on **Video Interop Server Pools** and choose **New Video Interop Server Pool**.
2. This will open up a **Create a new Video Interop Server Pool** wizard. Provide the Pool FQDN for the new Video Interop Server and select either **This pool has one server** or **This pool has multiple servers** based on your requirement, then press **Next**.

If you want to deploy a Video Interop Server pool to provide high availability, select **This pool has multiple servers**. Keep in mind with this option that:

- You must deploy DNS load balancing to support Video Interop Server pools.
- On the next page, for the **Define the computers in this pool** item, enter the **Computer FQDN** of each server in the pool into the text field, and then click **Add**. Repeat this step to add another Video Interop Server to the pool. When you have defined all the computers in the pool, press **Next**.

If you want to deploy only one Video Interop Server in the pool because you do not require high availability, then select **This pool has one server** and press **Next**.

3. Select the next hop pool/FE from the drop-down list and press **Next**.
4. Select an Edge Pool to associate with the VIS and press **Finish**.
5. Set a TCP or TLS port.

Select the newly added Video Interop Server from the left pane of Topology Builder, right click it and choose **Edit Properties**. Enable or Update the TCP or TLS port per your requirement and choose **OK**. Although by default TLS is added, only TCP has been fully tested with Cisco Unified Communications Manager (CallManager, or CUCM).

6. Add a video gateway. To do this, Expand Shared Components, right click on **Video Gateways** and select **New Video Gateway**.
7. Provide the video gateway FQDN or IP address. The video gateway could be in a subdomain or a different domain. The CUCM used by your system's VTCs serves as a video gateway.
8. Select either IPv4 or IPv6 as appropriate. You can use all configured IP addresses or limit service usage to selected IP addresses.
9. Select the listening port of the video gateway. Select the Transport protocol (TCP or TLS) and associate it with a Video Interop Server which is set up for a video SIP trunk. The Transport Protocol for the video gateway should match the Transport Protocol configured for the VIS.
10. A corresponding SIP Video trunk is added after the above step is completed. Right click on the SIP Video Trunk, and select the trunk that was just added. The video SIP Trunk name, associated Video Interop Server, SIP Transport protocol and port can all be changed.

**NOTE**

A Video Interop Server supports 1:N trunks. Hence multiple trunks can be added, which are associated with a single Video Interop Server, where each trunk terminates on a different Video Gateway. The limitation is that a particular Video Gateway has one and only one trunk that can be defined to the Skype for Business Server deployment.

11. Publish the Topology Document as described in [Create and publish new topology in Skype for Business Server 2015](#).

**NOTE**

To improve resiliency, you may want to configure a second Video Interop Server or VIS pool, or a backup Front End pool. See [Resiliency mechanisms](#) for more information.

All tasks performed using Topology Builder should now be complete. Proceed to installing the software on the new VIS server or servers.

## See also

[Deploy the VIS server role in Skype for Business Server](#)

[Plan for Video Interop Server in Skype for Business Server](#)

[Create and publish new topology in Skype for Business Server 2015](#)

# Deploy the VIS server role in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Deploy the Video Interop Server (VIS) role in Skype for Business Server.

To set up the VIS service on the server just created in Topology Builder, start the Skype for Business Server deployment wizard, press **Install or Update Skype for Business Server System** and follow these steps in the wizard:

1. Select **Install Local Configuration Store**.
2. Select **Setup or Remove Skype for Business Server Components**.
3. Select **Request, Install or Assign Certificates**.
4. Select **Start services**.

The software for this service is now installed and running. You may open the Services mmc tool to see if the **Skype for Business Server Video Interop Server** service is running along with other Skype for Business Server services. Next, you must configure the VIS server or pool.

## See also

[Configure the Video Interop Server in Skype for Business Server](#)

# Configure the Video Interop Server in Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Configure the Video Interop Server (VIS) role in Skype for Business Server.

Configure the settings that the VIS will associate with video trunks using Windows PowerShell. A video trunk configuration with global scope is created once the VIS service is installed. This video trunk configuration is applied by the VIS to all trunks which do not have video trunk configuration with a more specific scope. Note that the video trunk configuration is a collection of settings that is applicable to video trunks.

## Configure video trunk and dial plan

Use the following Windows PowerShell commands to specify the video trunk configuration and dial plan to be associated with the newly defined trunk(s) defined in the Topology Document between the VIS and all Video Gateways. All these settings can be set at the Global, Site, or service (Video Gateway) levels.

A dial plan with global scope is created per Skype for Business Server deployment. This dial plan is applied by VIS to all trunks which do not have any dial plan with more specific scope.

### Configure the VIS using Windows PowerShell

1. Create a new video trunk configuration (a collection of settings) to use on the trunk between the VIS and Cisco Unified Communications Manager (CallManager, or CUCM), using the following Windows PowerShell cmdlet:

```
New-CsVideoTrunkConfiguration -Identity "Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com" -
GatewaySendsRtcpForActiveCalls $false -GatewaySendsRtcpForCallsOnHold $false -
EnableMediaEncryptionForSipOverTls $true(or $false)
```

If there is an existing video trunk that needs to be modified, use the following Windows PowerShell cmdlet:

```
Set-CsVideoTrunkConfiguration -Identity "Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com" -
GatewaySendsRtcpForActiveCalls $false -GatewaySendsRtcpForCallsOnHold $false -
EnableMediaEncryptionForSipOverTls $true(or $false)
```

To view the settings associated with a particular video trunk configuration, use the following Windows PowerShell cmdlet:

```
Get-CsVideoTrunkConfiguration -Identity "Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com"
```

To remove a particular video trunk configuration, use the following Windows PowerShell cmdlet (note that the globally scoped video trunk configuration will be applied if there is not a more specifically scoped video trunk configuration for a particular trunk):

```
Remove-CsVideoTrunkConfiguration -Identity "Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com"
```

2. Establish a dial plan to associate with the trunk, using the following Windows PowerShell cmdlets:

```
New-CsDialPlan -Identity "Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com" -SimpleName
"TrunkTestDialPlan"
New-CsVoiceNormalizationRule -Identity
"Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com/SevenDigitRule" -Pattern '^(\d{7})$' -
Translation '+1425$1'
Get-CsDialPlan -Identity "Service:CUCMVIS1.CUCMInterop.contoso.com"
Remove-CsVoiceNormalizationRule -Identity "Service:VideoGateway:CUCMVIS1.CUCMInterop.contoso.com/Keep
All"
```

The **Remove-CsVoiceNormalizationRule** command is needed to override a default rule that will interfere with the expected VIS and CUCM interaction.

#### NOTE

[Remove-CsDialPlan](#) can be used to remove a dial plan.

For a video SIP Trunk call from a Video Gateway whose Request URI contains a non-E.164 number, VIS will read the name of the dial plan associated with the associated trunk, and will include the dial plan name in the phone context part of the Request URI in the Invite that VIS sends to the Front End. The Translation Application on the Front End then extracts and applies the normalization rules associated with the dial plan to the Request URI.

## Trunk configuration options

The Windows PowerShell cmdlets for video trunk configuration mentioned previously were new to Skype for Business Server 2015. The settings associated with video trunk configuration require a brief explanation.

**GatewaySendsRtcpForActiveCalls** This parameter determines whether RTCP packets are sent from the VTC to the VIS for active calls. An active call in this context is a call where media is allowed to flow in at least one direction. If **GatewaySendsRtcpForActiveCalls** is set to **True**, VIS can terminate a call if it does not receive RTCP packets for a period exceeding 30 seconds. The default is **True**.

**GatewaySendsRtcpForCallsOnHold** This parameter determines whether RTCP packets continue to be sent across the trunk for calls that have been placed on hold and no media packets are expected to flow in either direction. VIS can terminate the call, if there are no RTCP packets flowing from the VTC to VIS while the call is on Hold. The default is **True**. When the SIPTransport protocol is set to TCP, this setting is ignored.

**EnableMediaEncryptionForSipOverTls** This parameter enables or disables SRTP for media when the SIPTransport protocol is set to TLS. The default is **True**. When the SIPTransport protocol is set to TCP, this setting is ignored.

**EnableSessionTimer** This parameter enables or disables session timers on the VIS side for each SIP dialog associated with the video SIP trunk. The default is **False**.

**ForwardErrorCorrectionType** This parameter is used to determine if Forward Error Correction (FEC) for video streams is to be applied on the leg between the Video Interop Server and a Video Gateway. Setting **ForwardErrorCorrectionType** to "None" turns off FEC between VIS and Video Gateway/VTC. Setting **ForwardErrorCorrectionType** to "Cisco" enables FEC compatible with Video Gateways by Cisco, such as Cisco Unified Communications Manager (CUCM). The default is **None**.

## See also

[Configure CUCM for Interoperation with Skype for Business Server](#)

# Configure CUCM for Interoperation with Skype for Business Server

8/7/2019 • 4 minutes to read

**Summary:** Configure CUCM to work with Skype for Business Server.

## Caution

This capability is tested with Cisco Unified Communications Manager (CallManager, or CUCM) version 10.5 using Trunks setup over TCP only. Verify that the CUCM environment meets these criteria before proceeding.

The settings described here are meant only as examples of how CUCM can be configured to work with a VIS. Other settings and/or usages of alternate CUCM functionality could also be used to achieve the same result. No recommendation is implied as to the optimal configuration for a particular scenario.

A number of CUCM settings need to be confirmed or changed for interoperation with the VIS. Follow the procedures below in order to avoid missing required settings.

## Configure the CUCM

1. Log in to CUCM and navigate to Cisco Unified CM Administration->Call Routing->Class of Control->Partition.
2. In the Partition Configuration screen, enter the partition name and description and click on **Add New**.
3. Navigate to Cisco Unified CM Administration->Call Routing->Class of Control->Calling Search Space.
4. In the Calling Search Space Configuration screen, enter the name for the calling search space, and in Selected Partitions, enter the name of the partition you just created. Click **Save** when done.
5. Navigate to Cisco Unified CM Administration->System->Security->SIP Trunk Security Profile.
6. In the SIP Trunk Security Profile Configuration screen, set the SIP Trunk Security Profile Information options as shown, and click on **Add New**.

PARAMETER	RECOMMENDED SETTING
Name	SfBVideoInterop_SecurityProfile
Device Security Mode	Non Secure
Incoming Transport Type	TCP + UDP
Outgoing Transport Type	TCP
Incoming Port	5060

7. Navigate to Cisco Unified CM Administration->Device->Device Settings->SIP Profile.
8. In the SIP Profile Configuration screen, set the SIP Profile Information options as shown.

PARAMETER	RECOMMENDED SETTING
Name	SfBVideoInterop_SIPProfile

PARAMETER	RECOMMENDED SETTING
Description	SfBVideoInterop_SIPProfile

9. On the same screen, scroll down to the SDP Profile Information section. The **SDP Session-level Bandwidth Modifier for Early Offer and Re-invites** option is set by default to TIAS and AS. Change this option to TIAS only. If you leave this option at its default setting, Skype for Business Server will not understand the bandwidth modifier information in the SIP message. TIAS means Transport Independent Application Specific while AS means Application Specific. These are SIP options specified in RFC3890.
10. On the same screen, scroll down further. Under the SIP Profile's Trunk Specific Configuration, select **Early Offer Support for voice and video calls** and set it to the **Mandatory (insert MTP if needed)** option. This will enable CUCM to set up an outgoing SIP call with Early Offer. One new feature in CUCM 8.5 and beyond is that it supports outgoing call setup with Early Offer without requiring Media Termination Point (MTP).
11. Verify that in the SIP Options ping section, the box is checked next to "Enable OPTIONS Ping to monitor destination status for Trunks with Service Type 'None (Default)'."
12. When you are finished, click on **Add New**.
13. Navigate to Cisco Unified CM Administration->Device->Trunk.
14. Set the Device Protocol to SIP and press **Next**.
15. Under Device Information, Set the Device Name and Description (probably to something like SfBVideoInterop\_SIPTrunk), and set the Media Resource Group List to an MRGL that contains the right media resources.
16. Scroll down further. Media Termination Point (MTP) is not required for Video Calls, if it is not already unchecked, uncheck it. Check the option to **Run on all active Unified CM Nodes**. Please note that you should add all CUCM nodes to the Skype for Business Server configuration.
17. Scroll down further. Set the Inbound Calls and Connected Party Settings options as shown.

PARAMETER	RECOMMENDED SETTING
Calling Search Space	CSS_SfBVideoInterop
AAR Calling Search Space	CSS_SfBVideoInterop
Connected Party Transformation CSS	CSS_SfBVideoInterop

18. Scroll down further. Under the SIP Information Destination section of the SIP Trunk configuration, specify the VIS Pool's FQDN or the IP address of individual VIS servers in the pool (adding multiple entries). In the Destination Port specify the Port that VIS is listening at for connections from CUCM (the default is 6001). Also specify the SIP Trunk security profile and SIP profile you created earlier, as shown.

PARAMETER	RECOMMENDED SETTING
SIP Trunk Security Profile	SfBVideoInterop_SecurityProfile
Rerouting Calling Search Space	CSS_SfBVideoInterop
Out-of-Dialog Refer Calling Search Space	CSS_SfBVideoInterop

PARAMETER	RECOMMENDED SETTING
Subscribe Calling Search Space	CSS_SfBVideoInterop
SIP Profile	SfBVideoInterop_SIPProfile
DTMF Signaling Method	RFC 2833

19. Scroll down further. Set the Recording Information as appropriate for your system. It's fine to leave it set to **None**.
20. When you are finished, click on **Add New**.
21. Navigate to Cisco Unified CM Administration->Call Routing->Route/Hunt->Route pattern.
22. In the Route Pattern Configuration screen, enter the Pattern definition parameters shown below. Scroll down to the Called Party Transformations section and set the mask as shown, and then click on **Add New** when finished.

PARAMETER	RECOMMENDED SETTING
Route Pattern	7779999
Route Partition	SfBVideoInterop_RoutePartition
Description	Partition for SfBVideoInterop
Gateway/Route List	SfBVideoInterop_SIPTrunk
Called Party Transform Mask	+14257779999

23. Navigate to Cisco Unified CM Administration->Call Routing->SIP Route Pattern.
24. In the SIP Route Pattern Configuration screen, set the Pattern Definition options as shown, and click on **Add New**.

PARAMETER	RECOMMENDED SETTING
Pattern Usage	Domain Routing
IPv4 Pattern	contoso.com (leave blank if using IPv6)
IPv6 Pattern	contoso.com (leave blank if using IPv4)
Description	SIPRoute Pattern to mediavr
Route Partition	SfBVideoInterop_RoutePartition
SIP Trunk/Route List	SfBVideoInterop_SIPTrunk
Block Pattern checkbox	leave unchecked

25. If you have changed the audio or video bit rates from the default settings, you will need to return them to the defaults. To set the bit rate for Audio/Video calls, navigate to Cisco Unified CM Administration-



>System->Region Information->Region. The defaults are shown below for reference:

PARAMETER	RECOMMENDED SETTING
Region	Default
Audio Codec Preference List	System Default
Maximum Audio Bit Rate	64 kbps (G.722, G.711)
Maximum Session Bit Rate for Video Calls	200000 kbps
Maximum Session Bit Rate	2000000000 kbps

At this point the CUCM video gateway is configured to work with the VIS. Corresponding configuration will need to be done on each VTC you wish to integrate.

**NOTE**

To improve resiliency, you may want to configure this CUCM gateway to work with a second Video Interop Server or VIS pool. See [Resiliency mechanisms](#) for more information.

## See also

[Configure a VTC for Interoperation with Skype for Business Server](#)

# Configure a VTC for Interoperation with Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Configure the VTC devices to work with Skype for Business Server.

You will need to perform the following configuration customization procedures for each VTC that will connect to the Skype for Business VIS server through a SIP trunk and Cisco Unified Communications Manager (CallManager, or CUCM) video gateway.

The settings described here are meant only as examples of how CUCM can be configured to work with a VIS. Other settings and/or usages of alternate CUCM functionality could also be used to achieve the same result. No recommendation is implied as to the optimal configuration for a particular scenario.

## Configure a VTC registered with CUCM

1. Log in to the Cisco VTC device and navigate to Configuration->System Configuration->Provisioning.
2. Verify the following settings, correcting as needed:

PARAMETER	RECOMMENDED SETTING
Provisioning Mode	CUCM
ExternalManager Address	CUCM's FQDN
ExternalManager Domain	CUCM's domain

3. Navigate to Configuration->System Configuration->Network.

4. Verify the following settings, correcting as needed:

PARAMETER	RECOMMENDED SETTING
DNS Domain Name	CUCM's Domain name
DNS Server 1 Address	your desired DNS server address

5. Navigate to Configuration->System Configuration->Network Services. Ensure that H.323 mode is turned off and SIP mode is turned on.

6. These options are set automatically when the endpoint is registered with CUCM. Verify the following settings, correcting as needed:

PARAMETER	RECOMMENDED SETTING
H.323 Mode	Off
HTTP Mode	On
SIP Mode	On

PARAMETER	RECOMMENDED SETTING
Telnet Mode	On
WelcomeText	On
XMLAPI Mode	On

7. Navigate to Configuration->System Configuration->SIP.

8. Verify the following settings, correcting as needed:

PARAMETER	RECOMMENDED SETTING
Profile 1 - DefaultTransport	TCP
Profile 1 - Outbound	Off
Profile 1 - TlsVerify	On
Profile 1 - Type	Cisco
Profile 1 - URI	Automatically assigned at CUCM registration
Proxy 1 - Address	The host name of the CUCM

The VTC is now configured for interoperation. Before service can begin, there are final steps to perform on the CUCM side.

### Configure VTC devices on CUCM

1. Log in to CUCM and Navigate to Cisco Unified CM Administration->Device->Phone->Find.
2. Select the VTC device to be configured. Verify the following settings on the Phone Configuration screen, correcting as needed. Once these settings have been changed or verified, click on **Save**.

PARAMETER	RECOMMENDED SETTING
Device Information - Phone Button Template	Standard Cisco Telepresence Codec C40
Device Information - Common Phone Profile	Standard Common Phone Profile
Device Information - Calling Search Space	CSS_SfBVideoInterop
Device Information - AAR Calling Search Space	CSS_SfBVideoInterop
Device Information - Media Resource Group List	MRGL_SfBVideoInterop
Protocol Specific Information - Device Security Profile	Cisco Telepresence Codec C40
Protocol Specific Information - Rerouting Calling Search Space	CSS_SfBVideoInterop
Protocol Specific Information - SUBSCRIBE Calling Search Space	CSS_SfBVideoInterop

PARAMETER	RECOMMENDED SETTING
-----------	---------------------

Protocol Specific Information -SIP Profile	Standard SIP Profile for Telepresence Endpoint
--	--

- Once VTC configuration is saved, re-navigate to the Phone Configuration screen for the device. At the top of the screen in the Association group, click on the association for the Video Interop. This brings up the Directory Number Configuration screen.
- Verify the following settings, correcting as needed:

Make the appropriate changes as shown to the Directory Number Information and the Directory Number Settings.

PARAMETER	RECOMMENDED SETTING
Directory Number Information - Route Partition	SfBVideoInterop_RoutePartition
Directory Number Settings - Calling Search Space	CSS_SfBVideoInterop
MLPP Alternate Party and Confidential Access Level Settings - MLPP Calling Search Space	CSS_SfBVideoInterop
Line 1 on Device - Display (Caller ID)	As desired
Line 1 on Device - ASCII Display (Caller ID)	As desired

- When finished, scroll to the top of the screen and press **Save**.

Configuration is now complete for this VTC device. You will need to repeat this process for other VTC devices in your enterprise.

# Deploy Enterprise Voice in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to deploy Enterprise Voice for Skype for Business Server at a central site.

Use this topic to deploy Enterprise Voice at a central site. To deploy Enterprise Voice at a branch site, skip to [Deploying Branch Sites](#).

This section includes procedures for deployments in which a Mediation Server is collocated on each Front End Server or Standard Edition server, as recommended, and also for deployments with a stand-alone Mediation Server pool. You can skip the following content if you used Topology Builder to define and publish a topology that collocates a Mediation Server on each Front End Server or Standard Edition server, because Deployment Wizard already automatically installed the files for Mediation Server when you installed files for your Front End Server pool or Standard Edition server:

## In this section

- [Security and configuration prerequisites for Enterprise Voice in Skype for Business Server](#)
- [Deploy a Mediation Server in Topology Builder in Skype for Business Server](#)
- [Define a gateway in Topology Builder in Skype for Business Server](#)
- [Define additional trunks in Topology Builder in Skype for Business Server](#)
- [Install the files for Mediation Server in Skype for Business Server](#)
- [Configure trunks in Skype for Business Server](#)
- [Create or modify a translation rule for caller ID presentation in Skype for Business Server](#)
- [Create or modify a translation rule for called ID presentation in Skype for Business Server](#)
- [Create or modify a normalization rule in Skype for Business](#)
- [Create or modify a dial plan in Skype for Business Server](#)
- [Configure voice policies, PSTN usage records, and voice routes in Skype for Business](#)
- [Enable users for Enterprise Voice in Skype for Business Server](#)
- [Deploy advanced Enterprise Voice features in Skype for Business Server](#)
- [Deploy call management features in Skype for Business](#)

## See also

[Plan for Enterprise Voice in Skype for Business Server](#)

# Security and configuration prerequisites for Enterprise Voice in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn about the security and configuration prerequisites for Enterprise Voice in Skype for Business Server.

Before deploying Enterprise Voice, verify that your infrastructure meets the following security, user configuration, and scenario-specific hardware prerequisites.

## Administrative rights and certificate infrastructure

Before deploying, check the following:

- Administrators deploying Enterprise Voice should be members of the RTCUniversalServerAdmins group.
- Administrators performing the configuration tasks must have adequate rights:
  - **CsVoiceAdministrator:** This administrator role can perform voice configuration tasks, manage voice applications, and assign voice policies to end users.
  - **CsUserAdministrator:** This administrator role can manage user properties, such as enabling Enterprise Voice for a user. This administrator role can also assign per-user policies, with the exception of the archiving policy; move users; and manage common area phones and analog devices.
  - **CsAdministrator:** This administrator role can perform all of the tasks of CsVoiceAdministrator and CsUserAdministrator.
- Managed key infrastructure (MKI) is deployed and configured, by using either a Microsoft or a third-party certification authority (CA) infrastructure.

### NOTE

For details about certificate requirements in Skype for Business Server, see [Environmental requirements for Skype for Business Server 2015](#) or [Server requirements for Skype for Business Server 2019](#).

## User configuration

If you collocated the Mediation Server with each Front End pool or Standard Edition server during Front End deployment, user settings necessary for Enterprise Voice were configured automatically during installation of the files for those server roles.

If you are newly deploying the Enterprise Voice workload at this time, before you begin the deployment process, designate a primary phone number for each user who you plan to enable for Enterprise Voice. As the administrator, you are responsible for ensuring that this number is unique. Before implementation, all primary phone numbers must be normalized (correctly formatted) and copied to each user's **Line URI** property using Skype for Business Server Control Panel.

### NOTE

For examples of primary phone numbers required for Enterprise Voice deployment, see [Sample Normalization Rules](#).

## Next Steps: Install files or configure PSTN connectivity

After verifying software and environmental prerequisites for Enterprise Voice you can either:

- Install the Mediation Server, as described in [Deploy a Mediation Server in Topology Builder in Skype for Business Server](#), but only if you want to deploy a stand-alone Mediation Server or pool because Mediation Servers are installed as part of the Front End pool or Standard Edition server deployment process when collocated.
- Or, begin configuring settings to route calls for Enterprise Voice users, as described in [Configure trunks in Skype for Business Server](#).

# Deploy a Mediation Server in Topology Builder in Skype for Business Server

8/7/2019 • 4 minutes to read

**Summary:** Learn how to define and deploy a Mediation Server in Topology Builder in Skype for Business Server.

The Enterprise Voice workload, dial-in conferencing, and advanced Enterprise Voice applications (Response Group application, Call Park application, call admission control (CAC), and so on), are available in Front End pools. The functionality of the Mediation Server is built into the Front End Server. A separate stand-alone Mediation Server is not necessary.

The only exception is if you configure a SIP trunk to connect to a Session Border Controller for an Internet Telephony Service Provider. To connect your Enterprise Voice infrastructure to your SIP trunk provider, a separate Mediation Server must be deployed.

The connection between Skype for Business Server (either a Mediation Server collocated on a Front End pool or stand-alone Mediation Server) and a gateway is defined as a logical association called a trunk. The topics in this section describe how to define a trunk and how to deploy a stand-alone Mediation Server, if you connect to a SIP trunk.

## Define a Mediation Server in Topology Builder

You can add Mediation Server as a collocated role on a Front End pool, or define a separate standalone Mediation Server pool.

### To add a Mediation Server to a Front End pool

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server 2015 Topology Builder**.
2. In Topology Builder, in the console tree, expand the name of the site for which you want to define a Front End pool.
3. In the console tree, right-click the type of Front End pool you want, and then click **New Front End pool...**
4. Navigate through the **Define New Front End Pool** wizard until you reach the **Select collocated server roles** page.
5. In **Select collocated server roles**, check the option **Collocate Mediation Server**.

#### NOTE

If the type of Front End pool you selected is the Enterprise Edition, then the Mediation Server component will be installed on all the Front End Servers of that Front End pool.

#### NOTE

The **Next hop pool** used by the Mediation Server will be the Front End pool where the Mediation Server is collocated on.



**NOTE**

The **Edge pool** used by the Mediation Server will be the same Edge pool associated with the Front End pool where the Mediation Server is collocated on.

6. Click **Make Default** to use this Front End pool to route calls to the PSTN.
7. Click **Finish** when you are finished associating one or more peers to the Front End pool.

**NOTE**

Before you proceed to the next step in the Enterprise Voice deployment process, make sure that the Mediation Server pool (i.e. Front End pool with the Mediation Server component collocated) is using the FQDNs that you specified.

8. Right-click the **Skype for Business Server 2015** node, and then click **Publish Topology**.

**To add a standalone Mediation Server**

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server 2015 Topology Builder**.
2. In Topology Builder, in the console tree, expand the name of the site for which you want to define a Mediation Server.
3. In the console tree, right-click the **Mediation pools** node, and then click **Mediation Server pool**.
4. In **Define New Mediation Pool**, type the Mediation Server pool fully qualified domain name (FQDN).
5. Next, do one of the following:
  - If you want to deploy multiple Mediation Servers in the pool to provide high availability, then select **Multiple computer pool**.

**NOTE**

You must [deploy](#) to support Mediation Server pools that have multiple Mediation Servers.

- If you want to deploy only one Mediation Server in the pool because you do not require high availability, then select **Single computer pool**. Skip the following step.
6. If you selected **Multiple computer pool** in the previous step, on the **Define the computers in this pool** item, click **Computer FQDN**, type the FQDN of each server in the pool, and then click **Add**. Repeat this step for all other Mediation Servers that you want to add to the pool. When you have defined all the computers in the pool, click **Next**.
  7. On the **Select the next hop** page, click **Next hop pool**, click the FQDN of the Front End pool that will use this Mediation Server pool, and then click **Next**.
  8. On the **Select an Edge Server** page, do one of the following:
    - If you want to provide PSTN connectivity to external users enabled for Enterprise Voice, under **Select Edge Pool used by this Mediation Server**, click the FQDN of the Edge Server pool that will use this Mediation Server pool to provide PSTN connectivity to those external users, and then click **Next**.
    - If you do not plan to enable external users for Enterprise Voice, or if you do not want to provide

PSTN connectivity to users when they are outside the internal network, click **Next**.

9. Right-click the **Skype for Business Server 2015** node, and then click **Publish Topology**.

## Define the Mediation Server Listening Ports

Follow the steps in this topic to use Topology Builder to define the listening ports a Mediation Server or pool will accept incoming connections from a gateway peer.

### To Modify the Mediation Server Listening Ports

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server 2015 Topology Builder**.
2. In Topology Builder, in the console tree, expand the **Mediation pools** node, and right-click the Mediation Server previously created.
3. By default, the SIP listening ports on the Mediation Server are 5070 for TLS traffic from Skype for Business Server, and 5067 for TLS traffic from peers (such as gateways, PBXes, or SBCs). TCP port is disabled by default. You must enable TCP port if you have gateways that do not support TLS.
4. Specify the desired TLS or TCP listening port range the Mediation Server will accept incoming connections from PSTN gateways.

#### **NOTE**

Entering a TCP port range is not required if **Enable TCP port** is not checked. This setting is optional.

# Define a gateway in Topology Builder in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to define a PSTN gateway in Topology Builder in Skype for Business Server.

Follow these steps to use Topology Builder to define a peer with which you can associate a Mediation Server to provide connectivity to the public switched telephone network (PSTN) for users enabled for Enterprise Voice. A peer to the Mediation Server can be a PSTN gateway, an IP-PBX, or a Session Border Controller (SBC) for an Internet Telephony Service Provider (ITSP) to which you connect by configuring a SIP trunk.

## To define a peer for the Mediation Server

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server 2015 Topology Builder**.
2. Under Skype for Business Server, your site name, Shared Components, right-click the **PSTN Gateways** node, and then click **New PSTN Gateway**.
3. In **Define New IP/PSTN Gateway**, type the fully qualified domain name (FQDN) or IP address of the peer, and click **Next**.

### NOTE

If you specify Transport Layer Security (TLS) as the transport type, you must specify the FQDN instead of the IP address of the peer of the Mediation Server.

4. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and click **Next**.
5. Define a root trunk for the PSTN gateway. A trunk is a logical connection between a Mediation Server and a gateway uniquely identified by the tuple.  
`{Mediation Server FQDN, Mediation Server listening port (TLS or TCP) : gateway IP and FQDN, gateway listening port}`
  - When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
  - The root trunk cannot be removed until the associated PSTN gateway is removed.
6. Under **Listening Port for IP/PSTN Gateway**, type the listening port that the gateway, PBX, or SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway. (By default, the ports are 5066 for Transmission Control Protocol (TCP) and 5067 for Transport Layer Security (TLS) on a PSTN gateway, PBX or SBC. On a Survivable Branch Appliance at a branch site, the default ports are 5081 for TCP and 5082 for TLS.)
7. Under **SIP Transport Protocol**, click the transport type that the peer uses, and then click **OK**.

### NOTE

For security reasons, we strongly recommend that you deploy a peer to the Mediation Server that can use TLS.

8. Under **Associated Mediation Server**, select the Mediation Server pool to associate with the root trunk of

this PSTN Gateway.

9. Under **Associated Mediation Server port**, type the listening port that the Mediation Server will use for SIP messages from the gateway.

**NOTE**

With multiple trunk support in Skype for Business Server, you can define multiple SIP signaling ports on the Mediation Server for communication with multiple PSTN gateways. When defining a trunk, the **Associated Mediation Server port** must be within the range of the listening ports for the respective protocol allowed by the Mediation Server. This port range is defined under Skype for Business Server and Mediation Pools. Right-click the Mediation Server pool of interest, and select **Edit Properties**. Specify the port range in the **Listening ports** field.

10. Be sure that the peer you defined is running and using the FQDN or IP address that you specified. Then click **Finish**.
11. Right-click the **Skype for Business Server** node, and then click **Publish Topology**.

# Define additional trunks in Topology Builder in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to define an additional trunk between a Mediation Server and a gateway peer in Topology Builder in Skype for Business Server.

Follow these steps to define an additional trunk to which you can associate a peer with a Mediation Server. A peer provides users enabled for Enterprise Voice with connectivity to the Public Switched Telephone Network (PSTN). A peer can be a PSTN gateway, an IP-PBX, or a Session Border Controller (SBC) for an Internet Telephony Service Provider (ITSP).

A trunk is a logical connection between a Mediation Server and a gateway.

## NOTE

This topic assumes that you have setup a PSTN gateway and root trunk with at least one collocated or stand-alone Mediation Server or pool as described in [Define a gateway in Topology Builder in Skype for Business Server](#) in the Deployment documentation.

## To define an additional trunk between a Mediation Server and a gateway peer

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Skype for Business Server 2015**, and then click **Skype for Business Server 2015 Topology Builder**.
2. Under Skype for Business Server, your site name, **Shared Components**, right-click the **Trunks** node, and then click **New Trunk**.
  - a. In **Define New Trunk**, specify a friendly name to uniquely identify the trunk. You cannot have two trunks with the same name.

## NOTE

If you specify Transport Layer Security (TLS) as the transport type, you must specify the FQDN instead of the IP address of the peer of the Mediation Server.

3. Under **Associated PSTN gateway**, select the PSTN gateway peer to associate with this trunk. 5. Under **Listening Port for PSTN gateway**, type the listening port that the peer (PSTN gateway, IP-PBX, or SBC) will receive SIP messages from the Mediation Server that is to be associated with this trunk. The default peer ports are 5066 for Transmission Control Protocol (TCP) and 5067 for Transport Layer Security (TLS). The default Survivable Branch Appliance ports are 5081 for TCP and 5082 for TLS.
4. Under **SIP Transport Protocol**, click the transport type that the peer uses.

## NOTE

For security reasons, we strongly recommend that you deploy a peer to the Mediation Server that can use TLS.

5. Under **Associated Mediation Server**, select the Mediation Server pool to associate with the root trunk of this peer

- Under **Associated Mediation Server port**, type the listening port that the Mediation Server will receive SIP messages from the peer.

**NOTE**

With multiple trunk support in Skype for Business Server, two trunks with different trunk names cannot be configured with the same **Associated Mediation Server port** and **Listening Port for IP/PSTN gateway**

**NOTE**

With multiple trunk support in Skype for Business Server, multiple SIP signaling ports can be defined on the Mediation Server for communication with multiple peers. When defining a trunk, the **Associated Mediation Server port** number must be within the range of the listening ports for the respective protocol allowed by the Mediation Server. This port range is defined under Skype for Business Server and Mediation Server pools. Right-click the relevant Mediation Server pool, and select **Edit Properties**. Specify the port range in the **Listening ports** field.

- Click **OK**.

# Install the files for Mediation Server in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to install the files for Mediation Server in Skype for Business Server.

To successfully complete this procedure, you should be logged on to the server, at the minimum, as a local administrator and a domain user who has membership in at least the RTCUniversalReadOnlyAdmins group.

Use the steps in this topic to run Skype for Business Server Deployment Wizard to install the files for Mediation Server on a computer that you added to a Mediation Server pool after you have used Topology Builder to define and publish the pool. When installing files Mediation Server, you also install and assign the certificate required by each computer in a Mediation Server pool.

## NOTE

This topic assumes that you have already defined and published a stand-alone Mediation Server pool in your topology, as described in [Deploy a Mediation Server in Topology Builder in Skype for Business Server](#).

## To install the files for a stand-alone Mediation Server pool

1. From the installation media, right-click *<installation media>* \Setup\amd64\Setup.exe, and then click **Run as Administrator**.
2. On the **Installation Location** page, click **OK**.
3. On the **End User License Agreement** page, click **I accept**, and then click **OK**. (Required to continue.)
4. On the **Skype for Business Server Deployment Wizard** page, click **Install or Update Skype for Business Server System**.
5. Next to **Step 1: Install Local Configuration Store**, click **Run**, and then follow the instructions on the screen.
6. On the **Configure Local Replica of Central Management Store** page, accept the default **Retrieve directly from the Central Management Store**, and then click **Next**.
7. On the **Executing Commands** page, when the task status is shown as **Completed**, click **Finish**.
8. Next to **Step 2: Setup or Remove Skype for Business Server Components**, click **Run**, and then click **Next**.
9. On the **Executing Commands** page, when the task status is shown as **Completed**, click **Finish**.
10. Next to **Step 3: Request, Install or Assign Certificates**, click **Run**. Follow the instructions on the screen, accepting the default settings. The Mediation Server requires one certificate, and so you will run **Step 3** twice: once to issue the required certificate, and once more to assign it.
11. When the certificate has been issued and assigned correctly, beside **Step 4: Start Services**, click **Run**, and then follow the instructions on the screen.
12. When **Step 4** has completed successfully, restart the server, and log on to the server as a member of the DomainAdmins group.
13. On the computer where you are running Skype for Business Server Control Panel, verify on the **Topology**

page of Skype for Business Server Control Panel that the service status of the Mediation Server is shown as a green check mark. If a red X appears instead, select the Mediation Server. On the **Action** menu, click **Start All Services**.

If you added more than one computer to the Mediation Server pool, perform the steps in this procedure on all other computers in the Mediation Server pool. If you do not need to install files for Mediation Server for any other computers, then follow the procedures in [Configure trunks in Skype for Business Server](#) to configure settings for the trunk connection between this Mediation Server pool (or all Mediation Servers at a site) and its peer.



# Configure trunks in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to configure a trunk between a Mediation Server and peers for Enterprise Voice in Skype for Business Server.

As part of Enterprise Voice deployment, you can configure a trunk between a Mediation Server and one or more of the following peers to provide public switched telephone network (PSTN) connectivity for Enterprise Voice clients and devices in your organization:

- SIP trunk connection to an Internet telephony service provider (ITSP)
- PSTN gateway
- Private branch exchange (PBX)

For more details, see [Plan for PSTN connectivity in Skype for Business Server](#).

Skype for Business Server functionality supports multiple associations between gateways and Mediation Servers. These associations are made by defining a trunk, which is a logical association between a Mediation Server pool and a public switched telephone network (PSTN) gateway, Session Border Controller (SBC), or IP-PBX. Use the Topology Builder to associate gateways with Mediation Servers (that is, trunks).

- To assign or remove a trunk in Skype for Business Server, you must first define a trunk in Topology Builder. A trunk consists of the following association: Mediation Server fully qualified domain name (FQDN), the Mediation Server listening port, the gateway FQDN, and the gateway listening port.
- To configure multiple trunks, you can create multiple associations between the same gateway and the Mediation Server. This provides additional resiliency to the Enterprise Voice infrastructure, which is especially useful in private branch exchange (PBX) interoperational scenarios.

When a trunk is defined, it must be associated to a route. To associate a trunk to a route, you define a simple name for the trunk in Topology Builder. This simple name is used as the trunk name in the Skype for Business Server Control Panel, where trunks can be associated with routes. The simple trunk name is used as the gateway name from the Skype for Business Server Management Shell.

```
New-CsVoiceRoute -Identity <RouteId> -NumberPattern <String> -PstnUsages @{add="<UsageString>"} -  
PstnGatewayList @{add="<TrunkSimpleName>"}
```

The administrator must select a default trunk associated with a Mediation Server. From the Topology Builder, right-click the associated Mediation Server, and then click **Properties**. Specify the default gateway for the Mediation Server.

# Configure a trunk with media bypass in Skype for Business Server

8/7/2019 • 10 minutes to read

**Summary:** Configure a trunk with media bypass enabled for Skype for Business Server. This will let you minimize the number of Mediation Servers, presuming your SIP trunk provider supports it.

Follow these steps to configure a trunk with media bypass enabled. To configure a trunk with media bypass disabled, see [Configure a trunk without media bypass in Skype for Business Server](#).

Media bypass is useful when you want to minimize the number of Mediation Servers deployed. For more information, see [Plan for media bypass in Skype for Business](#)

We strongly recommend that you enable media bypass. However, before you enable media bypass on a SIP trunk, confirm that your qualified SIP trunk provider supports media bypass and is able to accommodate the requirements for successfully enabling the scenario. Specifically, the provider must have the IP addresses of servers in your organization's internal network.

## NOTE

Media bypass will not interoperate with every Public Switched Telephone Network (PSTN) gateway, IP-PBX, and Session Border Controller (SBC). Microsoft has tested a set of PSTN gateways and SBCs with certified partners. Media bypass is supported only with products and versions that are listed on the [Telephony Infrastructure for Skype for Business Server](#) page.

A trunk configuration as described below groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

## To configure a trunk with media bypass

1. Open Skype for Business Server Control Panel
2. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
3. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
  - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
  - Click **New**, and then select a scope for the new trunk configuration:
  - **Site trunk:** Choose the site for this trunk configuration from **Select a Site**, and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
  - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to. This trunk can be the root trunk or any additional trunks defined in Topology Builder. From **Select a Service**, click **OK**. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

**NOTE**

After you select the scope of the trunk configuration, it cannot be changed. > The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.

- Specify a value in **Maximum early dialogs supported**. This is the maximum number of forked responses a public switched telephone network (PSTN) gateway, IP-PBX, or ITSP Session Border Controller (SBC) can receive to an INVITE that it sent to the Mediation Server. The default value is 20.

**NOTE**

Before you change this value, consult your service provider or equipment manufacturer for details about the capabilities of your system.

- Select one of the following **Encryption support level** options:
  - Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
  - Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
  - Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
- Select the **Enable media bypass** check box if you want media to bypass the Mediation Server for processing by the trunk peer.

**IMPORTANT**

For media bypass to work successfully, the PSTN gateway, IP-PBX, or ITSP Session Border Controller must support certain capabilities. For details, see [Plan for media bypass in Skype for Business](#).

- Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a PSTN gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
- If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.

**NOTE**

If you disable this option while the **Enable media bypass** option is selected, additional settings are required. If the trunk peer does not support receiving SIP REFER requests from the Mediation Server and media bypass is enabled, you must also run the **Set-CsTrunkConfiguration** cmdlet to disable RTCP for active and held calls in order to support proper conditions for media bypass. Alternatively, you can select **Enable refer using third-party-call control** if you want transferred calls to be media bypassed, and the gateway does not support SIP REFER requests.

- (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Skype for Business Server endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
  - To select one or more records from a list of all PSTN usage records available in your Enterprise

Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.

- To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
- To define a new PSTN usage record and associate it with this trunk configuration, do the following:
  - a. Click **New**.
  - b. In the **Name** field, specify a descriptive name for the record that is unique.

**NOTE**

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

- c. Use one of the following methods to associate and configure routes for this PSTN usage record:
  - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
  - To remove a route from the PSTN usage record, select the route, and click **Remove**.
- To define a new route and associate it to this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
  - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**.
- d. Click **OK**.
  - To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
    - a. Select the PSTN usage record you want to edit, and click **Show details**.
    - b. Use one of the following methods to associate and configure routes for this PSTN usage record:
      - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
      - To remove a route from the PSTN usage record, select the route, and click **Remove**.
      - To define a new route and associate it to this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
      - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**.
- c. Click **OK**.

**IMPORTANT**

It is important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Skype for Business Server.

10. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, select the PSTN usage record, and click the up or down arrows.

#### **IMPORTANT**

The order in which PSTN usage records are listed in the trunk configuration is significant. Skype for Business Server traverses the list from top to down.

11. **Enable RTP Latching** should be selected to enable bypass media for clients behind a network address translation (NAT) or firewall and an SBC that supports latching.
12. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
13. **Enable forward P-Asserted-Identity data** should be selected to enable the P-Asserted-Identity (PAI) call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
14. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.
15. (Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls
  - To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
  - To define a new translation rule and associate it with the trunk, click **New**. For details about translation rules, see [Translation rules in Skype for Business Server](#).
  - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**.
  - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**.
  - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

#### **Caution**

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

16. (Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.
  - To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
  - To define a new translation rule and associate it with the trunk, click **New**. For details about translation rules, see [Translation rules in Skype for Business Server](#).
  - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**.

- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

**Caution**

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17. Make sure that the trunk's translation rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

**IMPORTANT**

Skype for Business Server traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

18. When you are finished configuring the trunk, click **OK**.
19. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

**NOTE**

Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

After you have configured the trunk, continue configuring media bypass by choosing between global media bypass options, as described in [Deploy media bypass in Skype for Business Server](#) in the Deployment documentation.

## See also

[Configure a trunk without media bypass in Skype for Business Server](#)

[Deploy media bypass in Skype for Business Server](#)

[Defining Translation Rules](#)

[Configure Media Bypass](#)

# Configure a trunk without media bypass in Skype for Business Server

8/7/2019 • 8 minutes to read

**Summary:** Configure a trunk without media bypass enabled for Skype for Business Server.

If you want to configure a trunk with media bypass disabled, follow these steps. If you want to configure a trunk with media bypass enabled, see [Configure a trunk with media bypass in Skype for Business Server](#).

A trunk configuration, as described below, groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

## To configure a trunk without media bypass

1. Open Skype for Business Server Control Panel.
  2. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
  3. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
    - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
    - Click **New**, and then select a scope for the new trunk configuration:
    - **Site trunk:** Choose the site for this trunk configuration in **Select a Site**, and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
    - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to in **Select a Service** and click **OK**. This trunk can be the root trunk, or any additional trunks defined in Topology Builder. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.
- NOTE**

After you select the scope of the trunk configuration, it cannot be changed. > The **Name** field is pre-populated with the name of the trunk configuration's associated site or service and cannot be changed.
4. Select one of the following **Encryption support level** options:
    - **Required:** Secure Realtime Transport Protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or Private Branch eXchange (PBX).
    - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
    - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
  5. Be sure that the **Enable media bypass** check box is cleared.

6. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a Public Switched Telephone Network (PSTN) gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
7. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.
8. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Skype for Business Server endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
  - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
  - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
  - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
    - a. Click **New**.
    - b. In the **Name** field, specify a descriptive name for the record that is unique.

**NOTE**

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

- c. Use one of the following methods to associate and configure routes for this PSTN usage record:
  - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
  - To remove a route from the PSTN usage record, select the route, and click **Remove**.
  - To define a new route and associate it to this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
  - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**.
- d. Click **OK**.
- To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
  - a. Select the PSTN usage record you want to edit, and click **Show details**.
  - b. Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see



[Create or modify a voice route in Skype for Business.](#)

- o To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**.
- c. Click **OK**.

**IMPORTANT**

It is important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Skype for Business Server.

9. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, select the PSTN usage record, and click the up or down arrows.

**IMPORTANT**

The order in which PSTN usage records are listed in the trunk configuration is significant. Skype for Business Server traverses the list from top to down.

10. **Enable RTP Latching** should be selected to enable bypass media for clients behind a NAT or firewall and an SBC that supports latching.
11. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
12. **Enable forward P-Asserted-Identity data** should be selected to enable PAI call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
13. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.
14. (Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls
- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
  - To define a new translation rule and associate it with the trunk, click **New**. For details about translation rules, see [Translation rules in Skype for Business Server](#).
  - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**.
  - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**.
  - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

**Caution**

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

15. (Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about translation rules, see [Translation rules in Skype for Business Server](#).
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

**Caution**

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

16. Make sure that the trunk's translation rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name, and then click the up or down arrow.

**IMPORTANT**

Skype for Business Server traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

17. When you are finished configuring the trunk, click **OK**.

18. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

**NOTE**

Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

## See also

[Configure a trunk with media bypass in Skype for Business Server](#)

[Defining Translation Rules](#)

# Create a new collection of trunk configuration settings in Skype for Business Server

8/7/2019 • 5 minutes to read

**Summary:** Learn how to create a new collection of trunk configuration settings by using the Skype for Business Server Control Panel.

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the Public Switched Telephone Network (PSTN) gateway, an IP-Public Branch eXchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which Realtime Transport Control Protocol (RTCP) packets are sent.
- Whether or not Secure Realtime Transport Protocol (SRTP) encryption is required on each trunk.

When you install Skype for Business Server, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only).

When creating SIP trunk configuration settings using Skype for Business Server Control Panel, the following options are available to you.

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Name	Identity	Unique identifier for the collection. This property is read-only; you cannot change the Identity of a collection of trunk configuration settings.
Description	Description	Provides a way for administrators to store addition information about the settings (for example, the purpose of the trunk configuration).
Maximum early dialogs supported	MaxEarlyDialogs	The maximum number of forked responses a PSTN gateway, IP-PBX, or SBC at the service provider can receive to an Invite that it sent to the Mediation Server.

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Encryption support level	SRTPMode	<p>Indicates the level of support for protecting media traffic between the Mediation Server and the PSTN Gateway, IP-PBX, or SBC at the service provider. For media bypass cases, this value must be compatible with the EncryptionLevel setting in the media configuration. Media configuration is set by using the <a href="#">New-CsMediaConfiguration</a> and <a href="#">Set-CsMediaConfiguration</a> cmdlets.</p> <p>Allowed values are:</p> <p>Required: SRTP encryption must be used.</p> <p>Optional: SRTP will be used if the gateway supports it.</p> <p>Not Supported: SRTP encryption is not supported and therefore will not be used.</p> <p>SRTPMode is used only if the gateway is configured to use Transport Layer Security (TLS). If the gateway is configured with Transmission Control Protocol (TCP) as the transport, SRTPMode is internally set to Not Supported.</p>
Refer support	Enable3pccRefer EnableReferSupport	<p>If set to <b>Enable sending refer to the gateway</b>, indicates that the trunk supports receiving Refer requests from the Mediation Server.</p> <p>If set to <b>Enable refer using third-party call control</b>, indicates that the 3pcc protocol can be used to allow transferred calls to bypass the hosted site. 3pcc is also known as "third party control," and occurs when a third-party is used to connect a pair of callers (for example, an operator placing a call from person A to person B).</p>
Enable media bypass	EnableBypass	<p>Indicates whether media bypass is enabled for this trunk. Media bypass can only be enabled if <b>Centralized media processing</b> is also enabled.</p>
Centralized media processing	ConcentratedTopology	<p>Indicates whether there is a well-known media termination point. (An example of a well-known media termination point would be a PSTN gateway where the media termination has the same IP as the signaling termination.)</p>
Enable RTP latching	EnableRTPLatching	<p>Indicates whether or not the SIP trunks support RTP latching. RTP latching is a technology that enables RTP/RTCP connectivity through a NAT (network address translator) device or firewall.</p>

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Enable forward call history	ForwardCallHistory	Indicates whether call history information will be forwarded through the trunk.
Enable forward P-Asserted-Identity data	ForwardPAI	Indicates whether the P-Asserted-Identity (PAI) header will be forwarded along with the call. The PAI header provides a way to verify the identity of the caller.
Enable outbound routing failover timer	EnableFastFailoverTimer	Indicates whether outbound calls that are not answered by the gateway within 10 seconds will be routed to the next available trunk; if there are no additional trunks then the call will automatically be dropped. In an organization with slow networks and gateway responses, that could potentially result in calls being dropped unnecessarily.
Associated PSTN usages	PSTNUsages	Collection of PSTN usages assigned to the trunk.
Translated number to test	N/A	Phone number that can be used to do an ad hoc test of the trunk configuration settings.
Associated translation rules	OutboundTranslationRulesList	Collection of phone number translation rules that apply to calls handled by Outbound Routing (calls routed to PBX or PSTN destinations).
Called number translation rules	OutboundCallingNumberTranslationRulesList	Collection of outbound calling number translation rules assigned to the trunk.
Phone number to test	N/A	Phone number that can be used to do an ad hoc test of the translation rules.
Calling number	N/A	Indicates that the phone number to test is the phone number of the caller.
Called number	N/A	Indicates that the phone number to test is the phone number of the person being called.

#### NOTE

The Skype for Business Server CsTrunkConfiguration cmdlets support additional properties not shown in Skype for Business Server Control Panel. For more information, see the help topic for the [New-CsTrunkConfiguration](#) cmdlet.

#### To create new trunk configuration settings by using Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel, click **Voice Routing**, and then click **Trunk Configuration**.
2. On the **Trunk Configuration** tab, click **New**, and then click **Site trunk** to create the new settings at the site

scope, or **Pool trunk** to create the new settings at the service scope.

3. In the **Select a Site** or the **Select a Service** dialog box (the dialog box that appears will depend on whether you are creating site-scoped or service-scoped settings) select the location for the new configuration settings and then click **OK**. If the dialog box is blank, that means there is no place to create the new settings; for example, if the **Select a Site** dialog box is blank that means that all of your sites have already been assigned a collection of trunk configuration sites, and each site (and each service) can only host one such collection. In that case, you can either delete the existing collection and create a new collection, or simply modify the existing collection.
4. In the **New Trunk Configuration** dialog, make the appropriate selections and then click **OK**.
5. The **State** property for the collection will be updated to **Uncommitted**. To commit the changes, and to delete the collection, click **Commit** and then click **Commit All**.
6. In the **Uncommitted Voice Configuration Settings** dialog box, click **OK**.
7. In the **Skype for Business Server Control Panel** dialog box click **OK**.

# Delete an existing collection of SIP trunk configuration settings in Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Learn how to delete a collection of trunk configuration settings by using the Skype for Business Server Control Panel.

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the Public Switched Telephone Network (PSTN) gateway, an IP-Public Branch eXchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which Realtime Transport Control Protocol (RTCP) packets are sent.
- Whether or not Secure Realtime Transport Protocol (SRTP) encryption is required on each trunk.

When you install Skype for Business Server, a global collection of SIP trunk configuration settings is created for you. This global collection of settings cannot be deleted. However, you can use the Skype for Business Server Control Panel or the [Remove-CsTrunkConfiguration](#) cmdlet to "reset" the properties in the global collection to their default values. For example, if you have set the Enable3pccRefer property to True, when you reset the global collection the Enable3pccRefer property will revert to its default value of False.

Administrators can also create custom trunk configuration settings at the site scope or at the service scope (for an individual PSTN gateway); these custom settings can be removed. When removing these custom settings keep the following in mind:

- If you remove service scope settings, then the SIP trunk managed by those settings will be managed by the settings applied to their site, if they exist. If site settings do not exist, those trunks will then be managed by the global collection of trunk configuration settings.
- If you remove site-scoped settings then any SIP trunks managed by those settings will now be managed by the global collection of trunk configuration settings.

## To remove trunk configuration settings with Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel, click **Voice Routing** and then click **Trunk Configuration**.
2. On the **Trunk Configuration** tab, select the collection of SIP trunk configuration settings to be deleted, click **Edit** and then click **Delete**. To delete multiple collections in the same operation, click the first collection to be deleted, then hold down the Ctrl key and click any additional collections that you want to remove.
3. The **State** property for the collection will be updated to **Uncommitted**. To commit the changes, and to delete the collection, click **Commit** and then click **Commit All**.
4. In the **Uncommitted Voice Configuration Settings** dialog box, click **OK**.
5. In the **Skype for Business Server Control Panel** dialog box click **OK**.
6. If you change your mind and decide not to delete the collection, click **Commit** and then click **Cancel All Uncommitted Changes**. When the **Skype for Business Server Control Panel** dialog box appears, click **OK**.

## Removing Trunk Configuration Settings by Using Skype for Business

# Server Management Shell Cmdlets

You can delete trunk configuration settings by using Skype for Business Server Management Shell and the **Remove-CsTrunkConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Skype for Business Server Management Shell.

## To remove a specified collection of settings

- The following command removes the trunk configuration settings applied to the Redmond site:

```
Remove-CsTrunkConfiguration -Identity site:Redmond
```

## To remove all the collections applied to the site scope

- This command removes all the trunk configuration settings applied to the service scope:

```
Get-CsTrunkConfiguration -Filter "service:*" | Remove-CsTrunkConfiguration
```

## To remove all the collections where media bypass is enabled

- The following command removes all the trunk configuration settings where media bypass has been enabled:

```
Get-CsTrunkConfiguration | Where-Object {$_.EnableBypass -eq $True} | Remove-CsTrunkConfiguration
```

For more information, see the help topic for the [Remove-CsTrunkConfiguration](#) cmdlet.



# Modify SIP trunk configuration settings in Skype for Business Server

8/7/2019 • 4 minutes to read

**Summary:** Learn how to modify SIP trunk configuration settings by using the Skype for Business Server Control Panel.

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the public switched telephone network (PSTN) gateway, an IP-Public Branch eXchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which Realtime Transport Control Protocol (RTCP) packets are sent.
- Whether or not Secure Realtime Transport Protocol (SRTP) encryption is required on each trunk.

When you install Skype for Business Server, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only). Any of these collections can later be modified using either Skype for Business Server Control Panel or Skype for Business Server Management Shell.

When modifying SIP trunk configuration settings using Skype for Business Server Control Panel, the following options are available to you.

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Name	Identity	Unique identifier for the collection. This property is read-only; you cannot change the Identity of a collection of trunk configuration settings.
Description	Description	Provides a way for administrators to store addition information about the settings (for example, the purpose of the trunk configuration).
Maximum early dialogs supported	MaxEarlyDialogs	The maximum number of forked responses a PSTN gateway, IP-PBX, or SBC at the service provider can receive to an Invite that it sent to the Mediation Server.

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Encryption support level	SRTPMode	<p>Indicates the level of support for protecting media traffic between the Mediation Server and the PSTN Gateway, IP-PBX, or SBC at the service provider. For media bypass cases, this value must be compatible with the EncryptionLevel setting in the media configuration. Media configuration is set by using the <a href="#">New-CsMediaConfiguration</a> and <a href="#">Set-CsMediaConfiguration</a> cmdlets.</p> <p>Allowed values are:</p> <p>Required: SRTP encryption must be used.</p> <p>Optional: SRTP will be used if the gateway supports it.</p> <p>Not Supported: SRTP encryption is not supported and therefore will not be used.</p> <p>SRTPMode is used only if the gateway is configured to use Transport Layer Security (TLS). If the gateway is configured with Transmission Control Protocol (TCP) as the transport, SRTPMode is internally set to Not Supported.</p>
Refer support	Enable3pccRefer EnableReferSupport	<p>If set to <b>Enable sending refer to the gateway</b>, indicates that the trunk supports receiving Refer requests from the Mediation Server.</p> <p>If set to <b>Enable refer using third-party call control</b>, indicates that the 3pcc protocol can be used to allow transferred calls to bypass the hosted site. 3pcc is also known as "third party control," and occurs when a third-party is used to connect a pair of callers (for example, an operator placing a call from person A to person B).</p>
Enable media bypass	EnableBypass	<p>Indicates whether media bypass is enabled for this trunk. Media bypass can only be enabled if <b>Centralized media processing</b> is also enabled.</p>
Centralized media processing	ConcentratedTopology	<p>Indicates whether there is a well-known media termination point. (An example of a well-known media termination point would be a PSTN gateway where the media termination has the same IP as the signaling termination.)</p>
Enable RTP latching	EnableRTPLatching	<p>Indicates whether or not the SIP trunks support RTP latching. RTP latching is a technology that enables RTP/RTCP connectivity through a NAT (network address translator) device or firewall.</p>

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Enable forward call history	ForwardCallHistory	Indicates whether call history information will be forwarded through the trunk.
Enable forward P-Asserted-Identity data	ForwardPAI	Indicates whether the P-Asserted-Identity (PAI) header will be forwarded along with the call. The PAI header provides a way to verify the identity of the caller.
Enable outbound routing failover timer	EnableFastFailoverTimer	Indicates whether outbound calls that are not answered by the gateway within 10 seconds will be routed to the next available trunk; if there are no additional trunks then the call will automatically be dropped. In an organization with slow networks and gateway responses, that could potentially result in calls being dropped unnecessarily.
Associated PSTN usages	PSTNUsages	Collection of PSTN usages assigned to the trunk.
Translated number to test	N/A	Phone number that can be used to do an ad hoc test of the trunk configuration settings.
Associated translation rules	OutboundTranslationRulesList	Collection of phone number translation rules that apply to calls handled by Outbound Routing (calls routed to PBX or PSTN destinations).
Called number translation rules	OutboundCallingNumberTranslationRulesList	Collection of outbound calling number translation rules assigned to the trunk.
Phone number to test	N/A	Phone number that can be used to do an ad hoc test of the translation rules.
Calling number	N/A	Indicates that the phone number to test is the phone number of the caller.
Called number	N/A	Indicates that the phone number to test is the phone number of the person being called.

#### NOTE

The Lync Server CsTrunkConfiguration cmdlets support additional properties not shown in Lync Server Control Panel. For more information, see the help topic for the [Set-CsTrunkConfiguration](#) cmdlet.

#### To modify SIP trunk configuration settings by using Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel, click **Voice Routing**, and then click **Trunk Configuration**.
2. On the **Trunk Configuration** tab, double-click the trunk configuration settings to be modified. Note that

you can only edit one collection of settings at a time. If you would like to make the same changes on multiple collections, use Windows PowerShell instead.

3. In the **Edit Trunk Configuration** dialog, make the appropriate selections and then click **OK**.
4. The **State** property for the collection will be updated to **Uncommitted**. To commit the changes, and to delete the collection, click **Commit** and then click **Commit All**.
5. In the **Uncommitted Voice Configuration Settings** dialog box, click **OK**.
6. In the **Skype for Business Server Control Panel** dialog box click **OK**.

# Test SIP trunk configuration settings in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to test SIP trunk configuration settings by using the Skype for Business Server Management Shell.

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the Public Switched Telephone Network (PSTN) gateway, an IP-Public Branch eXchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which Realtime Transport Control Protocol (RTCP) packets are sent.
- Whether or not Secure Realtime Transport Protocol (SRTP) encryption is required on each trunk.

When you install Skype for Business Server, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only). Administrators can also use the `Test-CsTrunkConfiguration` cmdlet to verify that a trunk can convert a number as dialed by a user to a number that can be handled by the gateway.

Trunk configuration settings can only be tested by using Windows PowerShell and the [Test-CsTrunkConfiguration](#) cmdlet. This cmdlet can be run either from the Skype for Business Server Management Shell or from a remote session of Skype for Business Server Management Shell.

## To test SIP trunk configuration settings

- This command verifies that the trunk configuration settings for the Redmond site can correctly convert the dialed number 4255551212.

```
$trunk = Get-CsTrunkConfiguration -Identity "site:Redmond"  
Test-CsTrunkConfiguration -DialedNumber 4255551212 -TrunkConfiguration $trunk
```

# View information about individual SIP trunks in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to view information about SIP trunks in Skype for Business Server.

SIP trunks are used to connect Skype for Business Server Voice over IP phone network with the Public Switched Telephone Network (PSTN). In previous version of the product, trunks were used to route outbound calls from a Mediation Server to a PSTN gateway and each gateway was limited to a single trunk. As a result, a PSTN gateway and a SIP trunk were essentially identical. For administrators, that meant they could view information about an individual SIP trunk simply by viewing information about the associated PSTN gateway.

In Skype for Business Server, however, multiple trunks can now be assigned to a single PSTN gateway; this means that gateways and trunks are no longer one and the same. In turn, that means that administrators must use the new [Get-CsTrunk](#) cmdlet in order to view information about an individual SIP trunk.

## To view information for all your SIP trunks

- The following command returns information about all the SIP trunks in use in your organization:

```
Get-CsTrunk
```

## To view information for a specific SIP trunk

- This command returns information only for the SIP trunk with the Identity PstnGateway:192.168.0.240:

```
Get-CsTrunk -Identity "PstnGateway:192.168.0.240"
```

## View information for all the SIP trunks assigned to a pool

- In this example, information is returned for all the SIP trunks assigned to the pool atl-cs-001.litwareinc.com:

```
Get-CsTrunk -PoolFqdn "atl-cs-001.litwareinc.com"
```

# Create or modify a translation rule for caller ID presentation in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to configure Caller ID by using the Skype for Business Server Control Panel.

With Skype for Business Server, the called party's phone number (that is, the phone number called) can be translated from E.164 format to the local dialing format that is required by the *trunk peer* (that is, the associated gateway, private branch exchange (PBX), or SIP trunk). To do this, you must define one or more translation rules to translate the Request URI before routing it to the trunk peer.

Skype for Business Server also gives you the option to also translate the calling party's phone number (that is, the phone number that the caller is calling from) from E.164 format to the local dialing format that is required by the trunk peer. For example, you can write a translation rule to remove +44 from the beginning of a dial string and replace it with 0144.

## To configure Caller ID by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
3. On the **Trunk Configuration** page, double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
4. To configure caller ID presentation:
  - To choose one or more rules from a list of all translation rules available in your Enterprise Voice deployment, click **Select**. In **Calling number translation rules**, click the rules that you want to associate with the trunk, and then click **OK**.
  - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see [Defining Translation Rules](#) in the Deployment documentation.
  - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see [Defining Translation Rules](#) in the Deployment documentation.
  - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see [Defining Translation Rules](#).
  - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

### Caution

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

# Create or modify a translation rule for called ID presentation in Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Learn how to define a translation rule by using the Build a Translation Rule tool in Skype for Business Server.

Follow these steps if you want to define a translation rule by entering a set of values in the **Build a Translation Rule** tool and enabling Skype for Business Server Control Panel to generate the corresponding matching pattern and translation rule for you. Alternatively, you can write a regular expression manually to define the matching pattern and translation rule. For details, see [Create or Modify a Translation Rule Manually](#).

## To define a rule by using the Build a Translation Rule tool

1. Open Skype for Business Server Control Panel.
2. To begin defining a translation rule, follow the steps in [Configure a trunk with media bypass in Skype for Business Server](#) through step 10 or [Configure a trunk without media bypass in Skype for Business Server](#) through step 9.
3. Under **Name** on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
4. (Optional) Under **Description**, type a description of the translation rule, for example US International long-distance dialing.
5. In the **Build a Translation Rule** section of the dialog box, enter values in the following fields:
  - **Starting digits:** (Optional) Specify the leading digits of numbers you want the pattern to match. For example, enter + in this field to match numbers in E.164 format (which begin with +).
  - **Length:** Specify the number of digits in the matching pattern and select whether you want the pattern to match numbers that are this length exactly, at least this length, or any length. For example, enter 11 and select At least in the drop-down list to match numbers that are at least 11 digits in length.
  - **Digits to remove:** (Optional) Specify the number of starting digits to be removed. For example, enter 1 to strip out the + from the beginning of the number.
  - **Digits to add:** (Optional) Specify digits to be prepended to the translated numbers. For example, enter 011 if you want 011 to be prepended to the translated numbers when the rule is applied.

The values you enter in these fields are reflected in the **Pattern to match** and **Translation rule** fields. For example, if you specify the preceding example values, the resulting regular expression in the **Pattern to match** field is:

```
^+(\d{9}\d+)$
```

The **Translation rule** field specifies a pattern for the format of translated numbers. This pattern has two parts:

- A value (for example, \$1) that represents the number of digits in the matching pattern
- (Optional) A value that you can prepend by entering it in the **Digits to add** field



Using the preceding example values, 011\$1 appears in the **Translation rule** field.

When this translation rule is applied, +441235551010 becomes 011441235551010.

6. Click **OK** to save the translation rule.
7. Click **OK** to save the trunk configuration.
8. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

#### NOTE

Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

### To define a translation rule manually

1. Open Skype for Business Server Control Panel
2. To begin defining a translation rule, follow the steps in [Configure a trunk with media bypass in Skype for Business Server](#) through step 10 or [Configure a trunk without media bypass in Skype for Business Server](#) through step 9.
3. In the **Name** field on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
4. (Optional) In **Description**, type a description of the translation rule, for example US International long-distance dialing.
5. Click **Edit** at the bottom of the **Build a Translation Rule** section.
6. Enter the following in **Type a Regular Expression**:
  - In **Match this pattern**, specify the pattern that will be used to match the numbers to be translated.
  - In **Translation rule**, specify a pattern for the format of translated numbers.

For example, if you enter `^+(\d{9}\d+)$` in **Match this pattern** and `011$1` in **Translation rule**, the rule will translate +441235551010 to 011441235551010.
7. Click **OK** to save the translation rule.
8. Click **OK** to save the trunk configuration.
9. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

#### NOTE

Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

## See also

[Configure a trunk with media bypass in Skype for Business Server](#)

[Configure a trunk without media bypass in Skype for Business Server](#)

[Publish pending changes to the voice routing configuration in Skype for Business](#)



# Create or modify a normalization rule in Skype for Business

8/7/2019 • 3 minutes to read

**Summary:** Learn how to define, create, and modify a normalization rule in Skype for Business Server.

Define, create, and modify normalization rules in Skype for Business Server.

## To define a normalization rule by using Build a Normalization Rule

1. Open Skype for Business Server Control Panel
2. (Optional) Follow the steps in [Create or modify a dial plan in Skype for Business Server](#) through step 11 or [Modify a Dial Plan](#) through step 10.
3. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example,5DigitExtension).
4. (Optional) In **Description**, type a description of the normalization rule (for example, "Translates 5-digit extensions").
5. In **Build a Normalization Rule**, enter values in the following fields:
  - **Starting digits** (Optional) Specify the leading digits of dialed numbers you want the pattern to match. For example, type425 if you want the pattern to match dialed numbers beginning with 425.
  - **Length** Specify the number of digits in the matching pattern and select whether you want the pattern to match this length exactly, match dialed numbers that are at least this length, or match dialed numbers of any length.
  - **Digits to remove** (Optional) Specify the number of starting digits to be removed from dialed numbers you want the pattern to match.
  - **Digits to add** (Optional) Specify digits to be added to dialed numbers you want the pattern to match.

The values you enter in these fields are reflected in **Pattern to match** and **Translation rule**. For example, if you leave **Starting digits** empty, type7 into the **Length** field and select **Exactly**, and specify 0 in **Digits to remove**, the resulting regular expression in the **Pattern to match** is:

```
^\d{7}$
```

6. In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers as follows:
  - A value that represents the number of digits specified in the matching pattern. For example, if the matching pattern is `^\d{7}$` then \$1 in the translation rule represents 7-digit dialed numbers.
  - (Optional) Type a value into the **Digits to add** field to specify digits to be prepended to the translated number (for example,+1425).

For example, if **Pattern to match** contains `^\d{7}$` as the pattern for dialed numbers and **Translation rule** contains `+1425$1` as the pattern for E.164 phone numbers, the rule normalizes 5550100 to +1425550100.

7. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.

- (Optional) Enter a number to test the normalization rule, and then click **Go**. The test results are displayed under **Enter a number to test**.

**NOTE**

You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see [Test Voice Routing](#).

- Click **OK** to save the normalization rule.
- Click **OK** to save the dial plan.
- On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

**NOTE**

Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

**To define a normalization rule manually**

- Open Skype for Business Server Control Panel
- (Optional) Follow the steps in [Create or modify a dial plan in Skype for Business Server](#).
- In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, name the normalization rule 5DigitExtension).
- (Optional) In **Description** field, type a description of the normalization rule (for example, "Translates 5-digit extensions").
- In **Build a Normalization Rule**, click **Edit**.
- Enter the following in **Type a Regular Expression**:
  - In **Match this pattern**, specify the pattern that you want to use to match the dialed phone number.
  - In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers.  
  
For example, if you enter `^\d{7}$` in **Match this pattern** and `+1425$1` in **Translation rule**, the rule normalizes 5550100 to +1425550100.
- (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
- (Optional) Enter a number to test the normalization rule and then click **Go**. The test results are displayed under **Enter a number to test**.
- Click **OK** to save the normalization rule.
- Click **OK** to save the dial plan.
- On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

**NOTE**

Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

# Create or modify a dial plan in Skype for Business Server

8/7/2019 • 8 minutes to read

**Summary:** Learn how to create or modify a dial plan by using the Skype for Business Server Control Panel.

## To create a dial plan

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
3. On the **Dial Plan** page, click **New** and select a scope for the dial plan:
  - **Site dial plan** applies to an entire site, except any users or groups that are assigned to a user dial plan. If you select **Site** for a dial plan's scope, you must choose the site from the **Select a Site** dialog box. If a dial plan has already been created for a site, the site does not appear in the **Select a Site** dialog box.
  - **Pool dial plan** can apply to a public switched telephone network (PSTN) gateway or a Registrar. If you select **Pool** for a dial plan's scope, choose the PSTN gateway or Registrar from the **Select a Service** dialog box. If a dial plan has already been created for a service (PSTN gateway or Registrar), the service does not appear in the list.
  - **User dial plan** can be applied to specified users or groups.

### NOTE

After you select the dial plan scope, it cannot be changed.

4. If you are creating a user dial plan, enter a descriptive name in the **Name** field on the **New Dial Plan** dialog box. After this name is saved, it cannot be changed.

### NOTE

For site dial plans, the **Name** field is prepopulated with the site name and cannot be changed.> For pool dial plans, the **Name** field is prepopulated with the PSTN gateway or Registrar name and cannot be changed.

5. The **Simple name** field is prepopulated with the same name that appears in the **Name** field. You can optionally edit this field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

### IMPORTANT

The **Simple name** must be unique among all dial plans in your deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), or an underscore (\_).> Characters **not supported** include spaces and Reserved characters as defined in RFC 3966 (<http://www.ietf.org/rfc/rfc3966.txt>). Reserved characters that are **not supported** in the **Simple Name** include the following:> ", " / " ? " . " @ " & " = " + " \$ " " , "

6. (Optional) In the **Description** field, you can type additional descriptive information about the dial plan.

- (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

**NOTE**

Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

- (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits (for example, 9) to get an external line. You can type in a prefix value of up to four characters (#, \*, and 0-9).

**NOTE**

If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

- Associate and configure normalization rules for the dial plan as follows:

- To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In **Select Normalization Rules**, highlight the rules you want to associate with the dial plan and then click **OK**.
- To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see [Create or modify a normalization rule in Skype for Business](#).
- To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**.
- To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**.
- To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

**NOTE**

Each dial plan must have at least one associated normalization rule. For information about how to determine all of the normalization rules a dial plan requires, see [Plan for outbound voice routing in Skype for Business Server](#) in the Planning documentation.

- Verify that the dial plan's normalization rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

**IMPORTANT**

Skype for Business Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones. > The default **Keep All** normalization rule  $^{\wedge}\{d{11}\}\$$  matches any 11-digit number. For example, if you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive  $^{\wedge}\{1425\}\{d{7}\}\$$  rule.

- (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under

**Enter a number to test.**

12. Click **OK**.
13. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

**NOTE**

Any time you create a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

**To modify a dial plan**

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

**NOTE**

The dial plan scope and name were set when the dial plan was created. They cannot be changed.

5. (Optional) In **Edit Dial Plan**, edit the **Simple name** field, which is prepopulated with the same name that appears in the **Name** field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

**IMPORTANT**

The **Simple name** must be unique among all dial plans within the Lync Server 2013 deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (\_).> Spaces are not allowed in the **Simple name** field.

6. (Optional) In the **Description** field, type descriptive information about the dial plan.
7. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

**NOTE**

Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

8. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits to get an external line (for example, 9). You can type in a prefix value of up to four characters (that is, #, \*, and 0-9).



**NOTE**

If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

9. Associate and configure normalization rules for the dial plan:

- To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In the **Select Normalization Rules** dialog box, highlight the rules that you want to associate with the dial plan and then click **OK**.
- To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see [Create or modify a normalization rule in Skype for Business](#).
- To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**.
- To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**.
- To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

**NOTE**

Each dial plan must have at least one associated normalization rule. For details about how to determine all of the normalization rules a dial plan requires, see [Plan for outbound voice routing in Skype for Business Server](#) in the Planning documentation.

10. Verify that the dial plan's normalization rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

**IMPORTANT**

Skype for Business Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones. > The default **Keep All** normalization rule  $^{\backslash d\{11\}}\$$  matches any 11-digit number. If, for example, you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive  $^{\{1425\}\backslash d\{7\}}\$$  rule.

11. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

**NOTE**

You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see [Testing Voice Routing](#).

12. Click **OK**.

13. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

**NOTE**

Any time you create or modify a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

## See also

[Publish pending changes to the voice routing configuration in Skype for Business](#)

# Configure voice policies, PSTN usage records, and voice routes in Skype for Business

8/7/2019 • 2 minutes to read

**Summary:** Learn how to configure voice policies, PSTN usage records, and voice routes in Skype for Business Server.

Voice policies, PSTN usage records, and voice routes are integrally related. You configure voice policies by selecting a set of calling features and then assigning the policy a set of PSTN usage records, which specify what rights are authorized for the users or groups who are assigned the voice policy. Voice routes are also assigned PSTN usage records, which serve to match routes with the users who are authorized to use them. That is, users can only place calls that use the routes for which they have a matching PSTN usage record.

The recommended workflow for a new Enterprise Voice deployment is to start by configuring a voice policy that includes the appropriate PSTN usage records, and then associate the appropriate routes to each PSTN usage record.

## NOTE

You can also create voice policies with *user* scope and assign them to individual users or groups.

For the detailed steps to perform each of these tasks, see the procedures in this section.

## In this section

- [Create or modify a voice policy and configure PSTN usage records in Skype for Business](#)
- [Configure voice mail escape in Skype for Business](#)
- [View PSTN usage records in Skype for Business](#)
- [Create or modify a voice route in Skype for Business](#)
- [Export or import a voice route configuration file in Skype for Business](#)
- [Publish pending changes to the voice routing configuration in Skype for Business](#)

# Create or modify a voice policy and configure PSTN usage records in Skype for Business

8/7/2019 • 18 minutes to read

**Summary:** Create or modify voice policies and configure PSTN usage records by using the Skype for Business Server Control Panel.

## NOTE

Each voice policy must have at least one associated Public Switched Telephone Network (PSTN) usage record. To see a listing of all PSTN usage records available in your Enterprise Voice deployment and view their properties, see [View PSTN usage records in Skype for Business](#).

## To create a voice policy

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Voice Routing** and then click **Voice Policy**.
3. On the **Voice Policy** page, click **New** and then select a scope for the new policy:
  - **Site policy** applies to an entire site, except any users or groups that are assigned to a user policy. If you select Site for a policy scope, choose the site from the **Select a Site** dialog box. If a voice policy has already been created for a site, the site does not appear in the **Select a Site** dialog box.
  - **User policy** can be applied to specified users or groups.
4. If the voice policy scope is User, enter a descriptive name for the policy in the **Name** field.

## NOTE

If the voice policy scope is Site, the **Name** field in **New Voice Policy** is prepopulated with the site name and cannot be changed.

5. (Optional) Enter additional descriptive information for the voice policy.
6. Select or clear the following check boxes to enable or disable each of the **Calling features** for this voice policy:
  - **Voice mail escape** prevents calls from being immediately routed to the user's mobile phone voice mail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range.

## NOTE

This feature is only configurable through the Skype for Business Server Management Shell

- **Call forwarding** enables users to forward calls to other phones and client devices. Skype for Business Server provides a significantly wider range of configuration options for call forwarding. For example, if an organization does not want to allow incoming calls to be forwarded externally to the PSTN, an administrator can apply a special voice policy to deploy this restriction. Enabled by

default.

- **Delegation** enables users to specify other users to send and receive calls on their behalf. In Skype for Business Server, a delegate can configure simultaneous ringing that enables incoming calls to his or her manager to ring all of the delegate's simultaneous ringing targets. This provides the delegate with greater flexibility in responding to calls directed to the manager. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls on hold and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on additional phones (for example, a mobile phone) or other endpoint devices. Skype for Business Server provides a significantly wider range of configuration options for simultaneous ringing. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN re-route** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the PSTN if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override call admission control policy decisions for a particular user. Disabled by default.

**NOTE**

The policy will be overridden only for incoming calls to the user and not for outgoing calls that are placed by the user. After the session is established, the bandwidth consumption will be accurately recorded. This setting should be used sparingly and should be reserved for appropriate call admission control decisions.

- **Malicious call tracing** enables users to report malicious calls (such as threats) by using the client UI, which in turn flags the calls in the Call Detail Records (CDRs). Disabled by default.
  - **Busy options** enables or disables Busy Options for the specified voice policy. Busy Options allows incoming calls to be routed to voice mail or rejected with a busy signal when the call's target user is on the phone. Busy Options is a new voice policy introduced in the July 2016 Cumulative Update. Checking this parameter enables Busy Options, and unchecking it disables Busy Options. For more information, see [Plan for Busy Options for Skype for Business Server](#) and [Install and configure Busy Options for Skype for Business Server](#).
7. To associate and configure PSTN usage records for this voice policy, do any of the following:
- To choose one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records that you want to associate with this voice policy, and then click **OK**.
  - To remove a PSTN usage record from this voice policy, highlight the record and click **Remove**.
  - To define a new PSTN usage record and associate it with this voice policy, do the following:
    - a. Click **New**.
    - b. In the **Name** field, enter a unique descriptive name for the record. For example, you may want to create a PSTN usage record named Redmond for full-time employees located in Redmond, and another named Redmond Temps for temporary employees.

**NOTE**

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

c. Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from the PSTN usage record, highlight the route, and then click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**.

d. Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:

a. Highlight the PSTN usage record that you want to edit, and then click **Show details**.

b. Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from this PSTN usage record, highlight the route, and then click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**.

c. Click **OK**.

8. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

**IMPORTANT**

The order in which PSTN usage records are listed in the voice policy is significant. Skype for Business Server traverses the list from the top down. We recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup.

9. To associate and configure PSTN usage records for call forwarding and simultaneous ringing in this voice policy, do any of the following:

- To use the same PSTN usage records for call forwarding and simultaneous ringing as this voice policy, select the option **Route using the call PSTN usages** from the drop-down menu.
- To allow call forwarding and simultaneous ringing to internal Skype for Business users only, select the option **Route to internal Skype for Business users only** from the drop-down menu. Calls will

not be forwarded to external PSTN numbers.

- To specify different PSTN usage records for call forwarding and simultaneous ringing than used for this voice policy, select the option **Route using custom PSTN usages** from the drop-down menu. This option displays a control to select existing PSTN usage records or create new PSTN usage records specifically for call forwarding and simultaneous ringing.
- To choose one or more records from a list of PSTN usage records for call forwarding and simultaneous ringing, click **Select**. Highlight the records that you want to associate with this call forwarding and simultaneous ringing policy, and then click **OK**.
- To remove a PSTN usage record from this call forwarding and simultaneous ringing policy, highlight the record and click **Remove**.
- To define a new PSTN usage record and associate it with this call forwarding and simultaneous ringing policy, do the following:
  - a. Click **New**.
  - b. In the **Name** field, enter a unique descriptive name for the record.

**NOTE**

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

- c. Use any of the following methods to associate and configure routes for this PSTN usage record:
    - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
    - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
    - To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
    - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**.
  - d. Click **OK**.
- To edit a PSTN usage record that is already associated with this voice policy, do the following:
    - a. Highlight the PSTN usage record you want to edit and click **Show details**.
    - b. Use any of the following methods to associate and configure routes for this PSTN usage record:
      - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
      - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
      - To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
      - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**.

c. Click **OK**.

10. (Optional) Enter a number to test the voice policy and click **Go**. The test results are displayed under **Translated number to test**.
11. Click **OK**.
12. On the **Voice Policy** page, click **Commit**, and then click **Commit all**.

#### NOTE

Any time you create or modify a voice policy, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

13. (Optional) Voicemail Escape detects that a call was immediately answered by the user's mobile phone voice mail, and disconnects the call to the mobile phone voice mail. This allows the call to continue to ring on the user's other endpoints giving the user the opportunity to answer the call. For details on how to configure a voice mail policy, see [Configure voice mail escape in Skype for Business](#).

#### To modify a voice policy

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Voice Routing**, and then click **Voice Policy**.
3. On the **Voice Policy** page, double-click a voice policy name.

#### NOTE

The scope and name were set when the voice policy was created. They cannot be changed.

4. (Optional) In **Edit Voice Policy**, enter additional descriptive information for the voice policy.
5. Select or clear the following check boxes to enable or disable each of the **Calling features**:
  - **Voice mail escape** prevents calls from being immediately routed to the user's mobile phone voice mail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range.

#### NOTE

This feature is only configurable through the Skype for Business Server Management Shell

- **Call forwarding** enables users to forward calls to other phones and client devices. Skype for Business Server provides a significantly wider range of configuration options for call forwarding. For example, if an organization does not want to allow incoming calls to be forwarded externally to the PSTN, an administrator can apply a special voice policy to deploy this restriction. Enabled by default.
- **Delegation** enables users to specify other users to send and receive calls on their behalf. In Skype for Business Server, a delegate can configure simultaneous ringing that enables incoming calls to his or her manager to ring all of the delegate's simultaneous ringing targets. This provides the delegate with greater flexibility in responding to calls directed to the manager. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.



- **Call park** enables users to park calls on hold, and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on additional phones (for example, a mobile phone) or other endpoint devices. Skype for Business Server provides a significantly wider range of configuration options for simultaneous ringing. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN re-route** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the PSTN if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override CAC policy decisions for a particular user. Disabled by default.

**NOTE**

The policy will be overridden only for incoming calls to the user and not for outgoing calls that are placed by the user. After the session is established, the bandwidth consumption will be accurately recorded. This setting should be used sparingly.

- **Malicious call tracing** enables users to report malicious calls (such as threats) using the client UI, which in turn flags the calls in the CDRs. Disabled by default.

6. To associate and configure PSTN usage records for this voice policy, do any of the following:

- To choose one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records that you want to associate with this voice policy, and then click **OK**.
- To remove a PSTN usage record from this voice policy, highlight the record and click **Remove**.
- To define a new PSTN usage record and associate it with this voice policy, do the following:

a. Click **New**.

b. In the **Name** field, enter a unique descriptive name for the record. For example, you may want to create a PSTN usage record namedRedmond for full-time employees located in Redmond, and another record namedRedmondTemps for temporary employees.

**NOTE**

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

c. Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from the PSTN usage record, highlight the route and click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
- To edit a route that is already associated with this PSTN usage record, highlight the route and click

### Show details.

d. Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:
  - a. Highlight the PSTN usage record that you want to edit and click **Show details**.
  - b. Use any of the following methods to associate and configure routes for this PSTN usage record:
    - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
    - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
    - To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
    - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**.
  - c. Click **OK**.

7. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

#### NOTE

The order in which PSTN usage records are listed in the voice policy is significant. Skype for Business Server traverses the list from the top down. We recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup.

8. To associate and configure PSTN usage records for call forwarding and simultaneous ringing in this voice policy, do any of the following:
- To use the same PSTN usage records for call forwarding and simultaneous ringing as this voice policy, select the option **Route using the call PSTN usages** from the drop-down menu.
  - To allow call forwarding and simultaneous ringing to internal Skype for Business users only, select **Route to internal Skype for Business users only** from the drop-down menu. Calls will not be forwarded to external PSTN numbers.
  - To specify different PSTN usage records for call forwarding and simultaneous ringing than those used for this voice policy, select the option **Route using custom PSTN usages** from the drop-down menu. This option displays a control to select existing PSTN usage records or to create new PSTN usage records, specifically for call forwarding and simultaneous ringing.
  - To choose one or more records from a list of PSTN usage records for call forwarding and simultaneous ringing, click **Select**. Highlight the records that you want to associate with this call forwarding and simultaneous ringing policy, and then click **OK**.
  - To remove a PSTN usage record from this call forwarding and simultaneous ringing policy, highlight the record and click **Remove**.
  - To define a new PSTN usage record and associate it with this call forwarding and simultaneous ringing policy, do the following:
    - a. Click **New**.

b. In the **Name** field, enter a unique descriptive name for the record.

**NOTE**

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

c. Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from the PSTN usage record, highlight the route and click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
- To edit a route that is already associated with this PSTN usage record, highlight the route, and then click **Show details**. For details, see [Modify a Voice Route](#).

d. Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:

a. Highlight the PSTN usage record that you want to edit and click **Show details**.

b. Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from this PSTN usage record, highlight the route and click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create or modify a voice route in Skype for Business](#).
- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see [Modify a Voice Route](#).

c. Click **OK**.

9. (Optional) Enter a number to test the voice policy and click **Go**. The test results are displayed under **Translated number to test**.

10. Click **OK**.

11. On the **Voice Policy** page, click **Commit**, and then click **Commit all**.

**NOTE**

Whenever you create or modify a voice policy, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

12. (Optional) Voicemail Escape detects that a call was immediately answered by the user's mobile phone voice mail, and disconnects the call to the mobile phone voice mail. This allows the call to continue to ring on the user's other endpoints giving the user the opportunity to answer the call. For details about how to

configure a voice mail policy, see [Configure voice mail escape in Skype for Business](#).

## See also

[View PSTN usage records in Skype for Business](#)

[Create or modify a voice route in Skype for Business](#)

[Publish pending changes to the voice routing configuration in Skype for Business](#)

[Configure voice mail escape in Skype for Business](#)

# Configure voice mail escape in Skype for Business

8/7/2019 • 2 minutes to read

**Summary:** Learn how to configure voice mail escape in Skype for Business Server by using the Skype for Business Server Management Shell.

When a user configures simultaneous ringing to a mobile phone, a caller will typically be routed to the user's personal voice mail if the mobile phone is turned off, out of battery power, or out of range. With Skype for Business Server, users can opt to have business-related calls routed to their corporate voice mail system. Specifically, a timer can be configured, and if the call is answered by the carrier's voice mail within the range of time defined, Skype for Business Server will disconnect from the carrier's voice mail system (and the user's personal voice mail), while the user's remaining endpoints in the corporate system continue to ring. This way, the caller is automatically routed to the user's corporate voice mail.

This configuration is performed using the Skype for Business Server Management Shell cmdlet, **Set-CsVoicePolicy**, at the voice policy level, with the following parameters.

## To configure voice mail escape

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Specify the following parameters to **Set-CsVoicePolicy**:
  - **EnableVoicemailEscapeTimer** - Enables or disables the escape timer.
  - **PSTNVoiceMailEscapeTimer** - Specifies the timeout value in milliseconds. The default value is 1500 milliseconds, and the value can range from 0 milliseconds to 8000 milliseconds.

## Example

```
Set-CsVoicePolicy UserVoicePolicy -EnableVoiceMailEscapeTimer $true - PSTNVoiceMailEscapeTimer 2000  
Set-CsVoicePolicy -Identity site:SitePolicy -EnableVoiceMailEscapeTimer $true -PSTNVoiceMailEscapeTimer 1500
```

## See also

[Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges](#)

# View PSTN usage records in Skype for Business

8/7/2019 • 2 minutes to read

**Summary:** Learn how to view PSTN usage records by using the Skype for Business Server Control Panel or the Skype for Business Server Management Shell.

A Public Switched Telephone Network (PSTN) usage record specifies a class of call (such as internal, local, or long distance) that can be made by various users or groups of users in an organization. For details, see [PSTN Usage Records](#) in the Planning documentation.

## To view a PSTN usage record by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Voice Routing** and then click **PSTN Usage**.
3. On the **PSTN Usage** page, highlight the PSTN usage record you want to view, click **Edit** and then click **Show details**.

### NOTE

A read-only page of the selected PSTN usage record shows the associated routes and associated voice policies.

## To view PSTN usage information by using Skype for Business Server Management Shell cmdlets

- To view information about all of your PSTN usages, type the following command in the Skype for Business Server Management Shell, and then press ENTER:

```
Get-CsPstnUsage
```

This command returns information similar to the following:

```
Identity : Global
Usage    : {Internal, Local, Long Distance}
```

## See also

[Create or modify a voice policy and configure PSTN usage records in Skype for Business](#)

# Create or modify a voice route in Skype for Business

8/7/2019 • 6 minutes to read

**Summary:** Learn how to create or modify a voice route in Skype for Business Server by using the Skype for Business Server Control Panel.

## To create a voice route by using the Skype for Business Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Routing**.
4. Click **Route**.
5. Click **New** to display the **New Voice Route** dialog box.
6. In **Name**, type a descriptive name for the voice route.
7. (Optional) In **Description**, type additional descriptive information for the voice route.
8. To specify the patterns that you want this route to accommodate, you can either use the **Build a pattern to match** tool to generate a regular expression, or write the regular expression manually.
  - To use the **Build a pattern to match** tool to generate a regular expression, enter values as follows. You can specify two types of pattern matching:
    - **Starting digits for numbers that you want to allow:** Enter prefix values that this route must accommodate (including the leading + if needed). For example, type +425, and then click **Add**. Repeat this for each prefix value that you want to include in the route.
    - **Exceptions:** If you want to specify one or more exceptions for a prefix value, highlight the prefix and click **Exceptions**. Type in one or more values for the matching patterns that you do *not* want this route to accommodate. For example, to exclude numbers starting with +425237 from the route, enter a value of +425237 in the **Exceptions** field, and then click **OK**.
    - To define the matching pattern manually, click **Edit** in the **Build a pattern to match** tool and then type in a .NET Framework regular expression to specify the matching pattern for destination phone numbers to which the route is applied. For details about how to write regular expressions, see "[.NET Framework Regular Expressions](#)".
9. Select **Suppress caller ID** if you do not want the ID of the phone making the outbound call to appear to the call recipient. If you select this option, you must specify an **Alternate caller ID** that will appear on the recipient's caller ID display.
10. To associate one or more trunks with the voice route, click **Add** and then select a trunk from the list.
11. To associate one or more Public Switched Telephone Network (PSTN) usages with the voice route, click **Select** and choose a record from the list of PSTN usage records that have been defined for your Enterprise Voice deployment.

**NOTE**

To view the properties of each of the available PSTN usage records, see [View PSTN usage records in Skype for Business](#). > To create or edit PSTN usage records, see [Create or modify a voice policy and configure PSTN usage records in Skype for Business](#)

12. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

**NOTE**

In contrast to a voice policy, where the order in which PSTN usage records are listed is important, the order in which PSTN usage records are listed in the voice route is insignificant. However, we recommend that you organize the list by frequency of use. For example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup. (Skype for Business Server traverses the list from the top down.)

13. (Optional) Type a value into the **Enter a translated number to test** field and click **Go**. The test results are displayed under the field.
14. Click **OK** to save the voice route.

**IMPORTANT**

Whenever you create a voice route, you must run the **Commit All** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#).

**To modify a voice route**

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Voice Routing**, and then click **Route**.
3. On the **Route** page, use either of the following methods to modify a voice route:
  - Click a voice route name, click **Edit**, and then click **Show details**.
  - Click a voice route name, click **Edit**, click **Copy**, and then click **Paste**. Click the new copy of the voice route that you just created, click **Edit**, and then click **Show details**.
4. In the **Name** field on the **Edit Voice Route** page, type a descriptive name for the voice route.
5. (Optional) In the **Description** field, type in additional descriptive information for the voice route.
6. To specify the patterns you want this route to accommodate, you can either use the **Build a pattern to match** tool to generate a regular expression, or write the regular expression manually.
  - To use the **Build a pattern to match** tool to generate a regular expression, enter values as follows. You can specify two types of pattern matching:
    - **Starting digits for numbers that you want to allow**: Enter prefix values that this route must accommodate (including the leading + if needed). For example, type +425 and then click **Add**. Repeat this for each prefix value that you want to include in the route.
    - **Exceptions**: If you want to specify one or more exceptions for a prefix value, highlight the prefix and click **Exceptions**. Type in one or more values for the matching patterns that you do *not* want this route to accommodate. For example, to exclude numbers starting with +425237 from the route, enter a value of +425237 in the **Exceptions** field, and then click **OK**.



- To define the matching pattern manually, click **Edit** in the **Build a pattern to match** tool and then type in a .NET Framework regular expression to specify the matching pattern for destination phone numbers to which the route is applied. For details about how to write regular expressions, see [".NET Framework Regular Expressions"](#).
7. Select **Suppress caller ID** if you do not want the ID of the phone that is making the outbound call to appear to the call recipient. If you select this option, you must specify an **Alternate caller ID** that will appear on the recipient's caller ID display.
  8. To associate one or more public switched telephone network (PSTN) trunks with the voice route, click **Add**, and then select a trunk from the list.
  9. To associate one or more PSTN usages with the voice route, click **Select** and choose a record from the list of PSTN usage records that have been defined for your Enterprise Voice deployment.

#### NOTE

To view the properties of each of the available PSTN usage records, see [View PSTN usage records in Skype for Business](#). > To create or edit PSTN usage records, see [Create or modify a voice policy and configure PSTN usage records in Skype for Business](#).

10. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

#### NOTE

In contrast to a voice policy where the order in which PSTN usage records are listed is important, the order of PSTN usage records in a voice route is insignificant. However, we recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup. (Skype for Business Server traverses the list from the top down.)

11. (Optional) Type a value into the **Enter a translated number to test** field and click **Go**. The test results are displayed under the field.
12. Click **OK**.
13. On the **Route** page, click **Commit**, and then click **Commit all**.

#### NOTE

Whenever you create or modify a voice route, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

## See also

[View PSTN usage records in Skype for Business](#)

[Create or modify a voice policy and configure PSTN usage records in Skype for Business](#)

[Publish pending changes to the voice routing configuration in Skype for Business](#)

# Export or import a voice route configuration file in Skype for Business

8/7/2019 • 2 minutes to read

**Summary:** Learn how to export or import a voice routing configuration file in Skype for Business Server by using the Skype for Business Server Control Panel.

If you want to save your voice routing configuration without publishing it, follow these steps to save and retrieve a snapshot of your voice routing configuration.

When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Skype for Business Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

If you have made any uncommitted changes to the settings on any page within the group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple sessions before you publish the changes.

## To export a voice routing configuration

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Export configuration**.
5. Specify a location and file name, and then click **Save**.

## To import a voice routing configuration

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Import configuration**.
5. Find the configuration file you want to import and then click **Open**.
6. Click **Commit**, and then click **Commit all**.

### NOTE

Whenever you import a voice configuration file, you must run the **Commit all** command to publish the configuration change. For details, see [Publish pending changes to the voice routing configuration in Skype for Business](#) in the Operations documentation.

# Publish pending changes to the voice routing configuration in Skype for Business

8/7/2019 • 2 minutes to read

**Summary:** Learn how to review, publish, or cancel voice routing configuration changes in Skype for Business Server by using the Skype for Business Server Control Panel.

After you make changes to any of the configuration settings in pages in the **Voice Routing** group, perform this procedure to review, publish, or cancel the pending changes.

## IMPORTANT

Be sure that only one user at a time modifies the Voice Routing configuration settings.

## NOTE

All pending changes must be published at the same time by running the **Commit all** command. You cannot selectively publish pending changes. Before you publish pending changes, run the **Review uncommitted changes** command and cancel any configuration changes that you do not want to publish.

## NOTE

If you navigate away from the pages in the **Voice Routing** group before committing pending changes, all pending changes will be lost. However, you can export the current configuration (including any pending changes) to a voice configuration file, and then import and publish the updated configuration. For details, see [Export or import a voice route configuration file in Skype for Business](#).

## To review, publish, or cancel voice routing configuration changes

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Routing**.
4. Make the configuration changes you want to the settings on each page of the **Voice Routing** group.
5. To review pending changes without publishing them, select **Review uncommitted changes** from the **Commit** menu.
6. If you want to cancel any of the pending changes, do one of the following:
  - Select **Cancel all uncommitted changes** from the **Commit** menu.
  - Navigate to the tab of the **Voice Routing** page that has pending changes you want to cancel, select the item with the pending changes, click **Commit**, and then click **Cancel selected changes**.
7. After you have reviewed all pending changes and canceled any that you do not want to publish, click **Commit**, and then click **Commit all**.

8. In the **Uncommitted Voice Configuration Settings** dialog box, which displays a list of all of the pending changes, click **OK**.

When Skype for Business Server Control Panel has committed the changes, the **Successfully published voice routing configuration** message appears.

# Enable users for Enterprise Voice in Skype for Business Server

8/7/2019 • 3 minutes to read

**Summary:** Learn how to enable users to make and receive calls by using Enterprise Voice in Skype for Business Server.

After you deploy Enterprise Voice or Call Via Work, you can use the following procedures to enable a user to make calls by using Enterprise Voice:

## NOTE

Of the following procedures, only the first can be performed by using Skype for Business Server Control Panel. For the remaining procedures, you can use only Skype for Business Server Management Shell.

- Enable the user account for Enterprise Voice.
- (Optional) Assign the user account a user-specific voice policy.
- (Optional) Assign the user account a user-specific dial plan.

## To enable a user account for Enterprise Voice

1. Log on to the computer as a member of the **RTCUniversalServerAdmins** group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to enable for Enterprise Voice.
6. On the **Edit** menu, click **Show details**.
7. On the **Edit Skype for Business Server User** page, under **Telephony**, click **Enterprise Voice**.
8. Click **Line URI**, and then type a unique, normalized phone number (for example, tel:+14255550200).
9. Click **Commit**.

To finish enabling a user for Enterprise Voice, be sure that the user is assigned a voice policy and a dial plan, whether global (assigned by default) or user-specific. By default, all users are assigned a global voice policy and dial plan. If a voice policy or dial plan exists at the site level for the site on which the user account is homed, those site policies will automatically apply to the user. To apply a per-user voice policy or dial plan to a user, you must run the **Grant-CsVoicePolicy** and **Grant-CsDialPlan** cmdlets. For details, see the following procedures in this topic.

## Voice Policy Assignment

Global and site-level voice policies are automatically assigned to all user accounts that are enabled for Enterprise

Voice. You can also create voice policies that apply to specific users or groups. These per-user policies must be explicitly assigned to the users or groups. If you want to use the global or site voice policy for all users who are enabled for Enterprise Voice, you can skip this section and continue to [Dial Plan Assignment](#) section later in this topic.

### To assign a user-specific voice policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. To assign an existing user voice policy to a user, run the following at the command prompt:

```
Grant-CsVoicePolicy -Identity <UserIdParameter> -PolicyName <String>
```

For example:

```
Grant-CsVoicePolicy -Identity "Bob Kelly" -PolicyName VoicePolicyJapan
```

In this example, the user with the display name Bob Kelly is assigned the voice policy with the name **VoicePolicyJapan**.

## Dial Plan Assignment

To complete user account configuration for either users of Enterprise Voice or users of dial-in conferencing, the user must be assigned a dial plan. User accounts will automatically use the global dial plan or, if one exists, the site-level dial plan, when you do not explicitly assign an existing per-user dial plan. If you want to use the global or site dial plan for all users who are enabled for Enterprise Voice, you can skip this section.

### To assign a user-specific dial plan

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. To assign a user-specific dial plan, run the following at the command prompt:

```
Grant-CsDialPlan -Identity <UserIdParameter> -PolicyName <String>
```

For example:

```
Grant-CsDialPlan -Identity "Bob Kelly" -PolicyName DialPlanJapan
```

In this example, the user with the display name Bob Kelly is assigned the user dial plan with the name **DialPlanJapan**.

# Deploy advanced Enterprise Voice features in Skype for Business Server

8/7/2019 • 2 minutes to read

Deploy advanced Enterprise Voice features in Skype for Business Server.

After you have configured basic Enterprise Voice functionality for your organization, you can optionally deploy one or more advanced Enterprise Voice features by following the procedures in this section.

- [Plan for media bypass in Skype for Business](#)
- [Plan for call admission control in Skype for Business Server](#)
- [Plan for emergency services in Skype for Business Server](#)

## In this section

- [Deploy network regions, sites and subnets in Skype for Business](#)
- [Deploy media bypass in Skype for Business Server](#)
- [Deploy call admission control in Skype for Business Server](#)
- [Deploy emergency services in Skype for Business Server](#)

# Deploy network regions, sites and subnets in Skype for Business

8/7/2019 • 10 minutes to read

Create or modify network regions, network sites, and associate network subnets in Skype for Business Server. All these are used for the advanced Enterprise Voice features: media bypass, call admission control, and location-based routing.

The advanced Enterprise Voice features are [call admission control](#), [media bypass](#), [location-based routing](#), and [E9-1-1](#). These features all require you to create network regions, network sites, and subnets. For example, all of these features require that each subnet in your topology be associated with a specific network site, and each network site must be associated with a network region. For more information on these terms, see [Network settings for the advanced Enterprise Voice features in Skype for Business Server](#).

Call admission control and E9-1-1 have additional configuration requirements for network sites:

- Call admission control requires that a bandwidth policy profile be specified for each site that is constrained by WAN bandwidth limitations. If you plan to deploy call admission control, you must [Create bandwidth policy profiles in Skype for Business Server](#) before you configure your network sites.
- E9-1-1 requires that a location policy be specified for each site. If you plan to deploy E9-1-1, you must [Create location policies in Skype for Business Server](#) before you configure your network sites.

## Create or modify a Network Region

If you have already created network regions for one of these features, you do not need to create new network regions; other advanced Enterprise Voice features will use those same network regions.

You may, however, need to modify an existing network region definition to apply feature-specific settings. For example, if you have created network regions for E9-1-1 (which do not require an associated central site) and you then deploy call admission control, you need to modify the network region definitions to specify a central site.

### To create a network region using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the New-CsNetworkRegion cmdlet to create network regions:

```
New-CsNetworkRegion -Identity <String> -CentralSite <String>
```

For example:

```
New-CsNetworkRegion -Identity NorthAmerica -CentralSite CHICAGO -Description "All North America Locations"
```

In this example, you created a network region called "NorthAmerica" that is associated with a central site with site ID CHICAGO.

3. To finish creating network regions for your topology, repeat step 2 with settings for each network region.

### To create a network region using Skype for Business Server Control Panel



1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click **Region**.
4. Click **New**.
5. On the **New Region** page, click **Name** and then type a name for the network region.
6. Click **Central site**, and then click a central site in the list.
7. Optionally, click **Description**, and then type additional information to describe this network site.
8. Click **Commit**.
9. To finish creating network regions for your topology, repeat steps 4 through 8 with settings for other regions.

#### To modify a network region using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the Set-CsNetworkRegion cmdlet to modify an existing network region:

```
Set-CsNetworkRegion -Identity <String> -CentralSite <String>
```

For example:

```
Set-CsNetworkRegion -Identity NorthAmerica -CentralSite CHICAGO -Description "North American Region"
```

In this example, you modified an existing network region called "NorthAmerica" (created using the procedures earlier in this topic) by changing the description. If a description existed for the "NorthAmerica" region, this command overwrites it with this value; if no description had been set, then this command sets it.

3. To modify other network regions, repeat step 2 with settings for other regions.

#### To modify a network region using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Region** navigation button.
4. In the table, click the network region that you want to modify.
5. Click **Edit**, and then click **Show details...**
6. On the **Edit Region** page, change the values for this network region's settings as appropriate.
7. Click **Commit**.
8. To finish modify network regions, repeat steps 4 through 7 with settings for other regions.

## Create or modify a network site

If you have already created network sites for one of these features, you do not need to create new network sites; other advanced Enterprise Voice features will use those same network sites. You may, however, need to modify an

existing network site definition to apply feature-specific settings. For example, if you created a network site for E9-1-1, you need to modify the network site during deployment of call admission control to apply a bandwidth policy profile.

### To create a network site by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the `New-CsNetworkSite` cmdlet to create network sites:

```
New-CsNetworkSite -NetworkSiteID <string>
```

For example:

```
New-CsNetworkSite -NetworkSiteID Chicago -Description "Corporate headquarters"-NetworkRegionID NorthAmerica
```

In this example, you created a network site called "Chicago" that is in the "NorthAmerica" network region.

#### NOTE

The NorthAmerica network region must already exist for this command to run successfully.

3. To finish creating network sites for your topology, repeat step 2 with settings for other sites.

### To create a network site by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Site** navigation button.
4. Click **New**.
5. On the **New Site** page, click **Name** and then type a name for the network site.
6. Click **Region**, and then click a region in the list.
7. Optionally, click **Bandwidth policy**, and then click a bandwidth policy in the list.

#### NOTE

Bandwidth policy is required only if you deploy call admission control at the site.

8. Optionally, click **Location policy**, and then click a location policy in the list.

#### NOTE

Location policy is required only if you deploy E9-1-1 at the site.

9. Optionally, click **Description**, and then type additional information to describe this network site.
10. Click **Commit**.
11. To finish creating network sites for your topology, repeat steps 4 through 10 with settings for other sites.

## To modify a network site by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the Set-CsNetworkSite cmdlet to modify network sites:

```
Set-CsNetworkSite -Identity <string>
```

For example:

```
Set-CsNetworkSite -Identity Albuquerque -NetworkRegionID NorthAmerica
```

In this example, the site called "Albuquerque" is moved to the "NorthAmerica" network region. To modify the network site configuration to deploy call admission control, E9-1-1, or media bypass, modify the network site settings by running the Set-CsNetworkSite cmdlet with the BWPolicyProfileID or LocationPolicy parameter, respectively.

### NOTE

Although the BypassID parameter exists for media bypass, we strongly recommend that you do not override automatically generated bypass IDs. You do not need to specify additional parameters to configure a network site for media bypass.

3. To finish modifying network sites for your topology, repeat step 2 with settings for other sites.

## To modify a network site by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Site** navigation button.
4. In the table, click the network site that you want to modify.
5. Click **Edit**, and then click **Show details...**
6. On the **Edit Site** page, change the values for this network site's settings as appropriate.
7. Click **Commit**.
8. To finish modify network sites, repeat steps 4 through 7 with settings for other sites.

## Associate a subnet with a network site

Every subnet in your network must be associated with a specific network site, because subnet information is used to determine the network site on which an endpoint is located while a new session is initiated. When the location of each party in a session is known, advanced Enterprise Voice features can apply that information to determine how to handle the call setup or routing.

All configured public IP addresses of the Audio/Video Edge Servers in your deployment must be added to your network configuration settings. These IP addresses are added as subnets with a mask of 32. The associated network site should correspond to the appropriate configured network site. For example, the public IP address that corresponds to the A/V Edge service in central site Chicago would be NetworkSiteID Chicago.

## To associate a subnet with a network site by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for**

**Business 2015**, and then click **Skype for Business Server Management Shell**.

2. Run the **New-CsNetworkSubnet** cmdlet to associate a subnet with a network site:

```
New-CsNetworkSubnet -SubnetID <String> -MaskBits <Int32> -NetworkSiteID <String>
```

For example:

```
New-CsNetworkSubnet -SubnetID 172.11.12.13 - MaskBits 20 -NetworkSiteID Chicago
```

In this example, you created an association between the subnet 172.11.12.13 and the network site "Chicago".

3. Repeat step 2 for all subnets in your topology.

### To associate subnets with network sites by importing a CSV file

1. Create a CSV file that includes all of the subnets you want to add. For example, create a file named **subnet.csv** with the following content:

```
IPAddress, mask, description, NetworkSiteID
```

```
172.11.12.0, 24, "NA:Subnet in Portland", Portland
```

```
172.11.13.0, 24, "NA:Subnet in Reno", Reno
```

```
172.11.14.0, 25, "EMEA:Subnet in Warsaw", Warsaw
```

```
172.11.15.0, 31, "EMEA:Subnet in Paris", Paris
```

2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following cmdlet to import **subnet.csv**, and then store its contents in the Lync Server management store:

```
import-csv subnet.csv | foreach {New-CsNetworkSubnet -Identity $_.IPAddress -MaskBits $_.mask -  
Description $_.description -NetworkSiteID $_.NetworkSiteID}
```

### To associate a subnet with a network site by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Subnet** navigation button.
4. Click **New**.
5. On the **New Subnet** page, click **Subnet ID**, and then type the first address in the IP address range defined by the subnet you want to associate with a network site.
6. Click **Mask**, and then type the bitmask to apply to the subnet.
7. Click **Network site ID**, and then select the site ID of the site to which you are adding this subnet.

#### NOTE

If you have not yet created network sites, this list will be empty. For details about the procedure, see [Create or Modify a Network Site](#). You can also retrieve site IDs for your deployment by running the **Get-CsNetworkSite** cmdlet. For details, see the Skype for Business Server Management Shell documentation.

8. Optionally, click **Description**, and then type additional information to describe this subnet.
9. Click **Commit**.

Repeat these steps to add other subnets to a network site.

#### NOTE

A Key Health Indicator (KHI) alert is raised, specifying a list of IP addresses that are present in your network but are either not associated with a subnet, or the subnet that includes the IP addresses is not associated with a network site. This alert will not be raised more than once within an 8-hour period.

The relevant alert information and an example are as follows:

**Source:** CS Bandwidth Policy Service (Core)

**Event number:** 36034

**Level:** 2

**Description:** The subnets for the following IP addresses: <List of IP Addresses> are either not configured or the subnets are not associated to a Network Site.

**Cause:** The subnets for the corresponding IP addresses are missing from the network configuration settings or the subnets are not associated to a network site.

**Resolution:** Add subnets corresponding to the list of IP addresses into the network configuration settings and associate every subnet to a network site.

For example, if the IP address list in the alert specifies 10.121.248.226 and 10.121.249.20, either these IP addresses are not associated with a subnet or the subnet they are associated with does not belong to a network site. If 10.121.248.0/24 and 10.121.249.0/24 are the corresponding subnets for these addresses, you can resolve this issue as follows:

1. Be sure that IP address 10.121.248.226 is associated with the 10.121.248.0/24 subnet and IP address 10.121.249.20 is associated with the 10.121.249.0/24 subnet.
2. Be sure that the 10.121.248.0/24 and 10.121.249.0/24 subnets are each associated with a network site.

## See also

[New-CsNetworkRegion](#)

[Get-CsNetworkRegion](#)

[Set-CsNetworkRegion](#)

[Remove-CsNetworkRegion](#)

[New-CsNetworkSubnet](#)

[Get-CsNetworkSubnet](#)

Set-CsNetworkSubnet

Remove-CsNetworkSubnet

# Deploy call admission control in Skype for Business Server

8/7/2019 • 2 minutes to read

Call admission control (CAC) is a solution that determines whether a real-time session can be established based on the available bandwidth to help prevent poor audio/video quality for users on congested networks. For more information, see [Plan for call admission control in Skype for Business Server](#).

## To deploy Call Admission Control

1. Gather all of the required information for your enterprise network topology, as described in [Example: Gathering requirements for call admission control in Skype for Business Server](#).
2. If you have not done so already, you must define network regions and sites, and associate subnets with network sites. For details, see [Deploy network regions, sites and subnets in Skype for Business](#).
3. Create bandwidth policy profiles, as detailed in [Create bandwidth policy profiles in Skype for Business Server](#)
4. Create network region links, as detailed in [Create network region links in Skype for Business Server](#).
5. Create network inter-region routes, as detailed in [Create network interregional routes in Skype for Business Server](#).
6. Create network intersite policies, as detailed in [Create network intersite policies in Skype for Business Server](#).
7. Enable call admission control, as detailed in [Enable call admission control in Skype for Business Server](#).
8. Check a few final settings, to make sure everything is set up correctly. For details, see [Call admission control deployment: final checklist for Skype for Business Server](#).

# Create bandwidth policy profiles in Skype for Business Server

8/7/2019 • 2 minutes to read

Create or modify bandwidth policies, which are used by Enterprise Voice call admission control in Skype for Business Server.

Bandwidth policies define limitations on bandwidth usage for real-time audio and video modalities. Bandwidth policies are applied to bandwidth policy profiles, which can be applied to multiple network sites for call admission control.

For guidelines about what bandwidth limits you should set in your CAC deployment, see [Plan for call admission control in Skype for Business Server](#).

The example policies created in the following procedure set limits for overall audio traffic, individual audio sessions, overall video traffic, and individual video sessions. For example, the 5Mb\_Link bandwidth policy profile sets the following limits:

- Audio Limit: 2,000 kbps
- Audio Session Limit: 200 kbps
- Video Limit: 1,400 kbps
- Video Session Limit: 700 kbps

## NOTE

The minimum Audio Session Limit value is 40 kbps. The minimum Video Session Limit value is 100 kbps.

## To create bandwidth policy profiles by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. For each bandwidth policy profile that you want to create, run the New-CsNetworkBandwidthPolicyProfile cmdlet. For example, run:

```
New-CsNetworkBandwidthPolicyProfile -Identity 5Mb_Link -Description "BW profile for 5Mb links" -  
AudioBWLimit 2000 -AudioBWSessionLimit 200 -VideoBWLimit 1400 -VideoBWSessionLimit 700
```

```
New-CsNetworkBandwidthPolicyProfile -Identity 10Mb_Link -Description "BW profile for 10Mb links" -  
AudioBWLimit 4000 -AudioBWSessionLimit 200 -VideoBWLimit 2800 -VideoBWSessionLimit 700
```

```
New-CsNetworkBandwidthPolicyProfile -Identity 50Mb_Link -Description "BW profile for 50Mb links" -  
AudioBWLimit 20000 -AudioBWSessionLimit 200 -VideoBWLimit 14000 -VideoBWSessionLimit 700
```

```
New-CsNetworkBandwidthPolicyProfile -Identity 25Mb_Link -Description "BW profile for 25Mb links" -  
AudioBWLimit 10000 -AudioBWSessionLimit 200 -VideoBWLimit 7000 -VideoBWSessionLimit 700
```



## To create bandwidth policy profiles by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Policy Profile** navigation button.
4. Click **New**.
5. On the **New Policy Profile** page, click **Name** and then type a name for the bandwidth policy profile.
6. Click **Audio limit**, and then type in the maximum number of kbps to allow for all audio sessions combined.
7. Click **Audio session limit**, and then type in the maximum number of kbps to allow for each individual audio session.
8. Click **Video limit**, and then type in the maximum number of kbps to allow for all video sessions combined.
9. Click **Video session limit**, and then type in the maximum number of kbps to allow for each individual video session.
10. Optionally, click **Description**, and then type additional information to describe this bandwidth policy profile.
11. Click **Commit**.
12. To finish creating bandwidth policy profiles for your topology, repeat steps 4 through 11 with settings for other bandwidth policy profiles.

## See also

[New-CsNetworkBandwidthPolicyProfile](#)

[Get-CsNetworkBandwidthPolicyProfile](#)

[Set-CsNetworkBandwidthPolicyProfile](#)

[Remove-CsNetworkBandwidthPolicyProfile](#)

# Create network region links in Skype for Business Server

8/7/2019 • 2 minutes to read

Create or modify network region links, which are used by Enterprise Voice call admission control in Skype for Business Server.

Regions within a network are linked through physical WAN connectivity. A network region link creates a link between two regions configured for Call Admission Control (CAC) and sets the bandwidth limitations on audio and video traffic between these regions.

The example topology has a link between the North America and APAC regions, and a link between the EMEA and APAC regions. Each of these region links is constrained by WAN bandwidth, as described in Region Link Bandwidth Information table in [Example: Gathering requirements for call admission control in Skype for Business Server](#).

## To create network region links by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the `New-CsNetworkRegionLink` cmdlet to create the region links and apply appropriate bandwidth policy profiles. For example, run:

```
New-CsNetworkRegionLink -NetworkRegionLinkID NA-EMEA-LINK -NetworkRegionID1 NorthAmerica -  
NetworkRegionID2 EMEA -BWPolicyProfileID 50Mb_Link
```

```
New-CsNetworkRegionLink -NetworkRegionLinkID EMEA-APAC-LINK -NetworkRegionID1 EMEA -NetworkRegionID2  
APAC -BWPolicyProfileID 25Mb_Link
```

## To create network region links by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Region Link** navigation button.
4. Click **New**.
5. On the **New Region Link** page, click **Name** and then type a name for the network region link.
6. Click **Network Region #1**, and then click the network region in the list that you want to link to Network Region #2.
7. Click **Network Region #2**, and then click a network region in the list that you want to link to Network Region #1.
8. Optionally, click **Bandwidth policy**, and then select the bandwidth policy profile that you want to apply to the network region link.

**NOTE**

Apply a bandwidth policy only if the network region link is bandwidth-constrained and you want to use CAC to control media traffic on that link.

9. Click **Commit**.
10. To finish creating network region links for your topology, repeat steps 4 through 9 with settings for other regions.

## See also

[New-CsNetworkRegionLink](#)

[Get-CsNetworkRegionLink](#)

[Set-CsNetworkRegionLink](#)

[Remove-CsNetworkRegionLink](#)

# Create network interregional routes in Skype for Business Server

8/7/2019 • 2 minutes to read

Create or modify network interregional routes, which are used by Enterprise Voice call admission control in Skype for Business Server.

A network interregional route defines the route between a pair of network regions. Each pair of network regions in your call admission control deployment requires a network interregional route. This enables every network region within the deployment to access every other region.

While region links set bandwidth limitations on the connections between regions, an interregional route determines which linked path the connection will traverse from one region to another.

In the example topology, network interregional routes must be defined for each of the three region pairs: North America/EMEA, EMEA/APAC, and North America/APAC.

## To create network interregional routes by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the **New-CsNetworkInterRegionRoute** cmdlet to define the required routes. For example, run:

```
New-CsNetworkInterRegionRoute -Identity NorthAmerica_EMEA_Route -NetworkRegionID1 NorthAmerica -  
NetworkRegionID2 EMEA -NetworkRegionLinkIDs "NA-EMEA-LINK"
```

```
New-CsNetworkInterRegionRoute -Identity NorthAmerica_APAC_Route -NetworkRegionID1 NorthAmerica -  
NetworkRegionID2 APAC -NetworkRegionLinkIDs "NA-EMEA-LINK, EMEA-APAC-LINK"
```

```
New-CsNetworkInterRegionRoute -Identity EMEA_APAC_Route -NetworkRegionID1 EMEA -NetworkRegionID2 APAC -  
NetworkRegionLinkIDs "EMEA-APAC-LINK"
```

### NOTE

The North America/APAC network interregional route requires two network region links because there is no direct network region link between them.

## To create network interregional routes by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Region Route** navigation button.
4. Click **New**.
5. On the **New Region Route** page, click **Name** and then type a name for the network interregional route.
6. Click **Network Region #1**, and then click a network region in the list that you want to route to Network Region #2.

7. Click **Network Region #2**, and then click a network region in the list that you want to route to Network Region #1.
8. Click **Add** beside the **Network Region Links** field, and then add a network region link that will be used in the network interregional route.

**NOTE**

If you are creating a route for two network regions that do not have a direct network region link between them, you must add all the necessary links to complete the route. For example, the North America/APAC network interregional route requires two network region links because there is no direct network region link between them.

9. Click **Commit**.
10. To finish creating network interregional routes for your topology, repeat steps 4 through 9 with settings for other network interregional routes.

## See also

[New-CsNetworkInterRegionRoute](#)

[Get-CsNetworkInterRegionRoute](#)

[Set-CsNetworkInterRegionRoute](#)

[Remove-CsNetworkInterRegionRoute](#)

# Create network intersite policies in Skype for Business Server

8/7/2019 • 2 minutes to read

Create network inter-site policies, which are used by Enterprise Voice call admission control in Skype for Business Server.

A network inter-site policy defines bandwidth limitations between sites that have direct WAN links between them.

## IMPORTANT

A network inter-site policy is required *only* if there is a direct cross link between two network sites.

In the example topology North America region, there is a direct link between the Reno and Albuquerque sites. These two sites require an inter-site policy that applies an appropriate bandwidth policy profile. The following example applies the 20Mb\_Link profile.

### To create a network inter-site policy

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the `New-CsNetworkInterSitePolicy` cmdlet to create network inter-site policies and apply an appropriate bandwidth policy profile for two sites that have a direct cross link. For example, run:

```
New-CsNetworkInterSitePolicy -InterNetworkSitePolicyID Reno_Albuquerque -NetworkSiteID1 Reno -  
NetworkSiteID2 Albuquerque -BWPolicyProfileID 20Mb_Link
```

3. Repeat step 2 as needed to create network inter-site policies for all network sites pairs that have a direct cross link.

## See also

[New-CsNetworkInterSitePolicy](#)

[Get-CsNetworkInterSitePolicy](#)

[Set-CsNetworkInterSitePolicy](#)

[Remove-CsNetworkInterSitePolicy](#)

# Enable call admission control in Skype for Business Server

8/7/2019 • 2 minutes to read

Enable call admission control in Skype for Business Server Enterprise Voice.

After you have configured your network settings for call admission control deployment, you must enable CAC to put your bandwidth policies into effect.

## To enable call admission control by using Skype for Business Server Management Shell

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the Set-CsNetworkConfiguration cmdlet to enable CAC in your network. For example, run:

```
Set-CsNetworkConfiguration -EnableBandwidthPolicyCheck 1
```

If you want to disable CAC in your network, run the following:

```
Set-CsNetworkConfiguration -EnableBandwidthPolicyCheck 0
```

## To enable call admission control by using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Global** navigation button.
4. Click **Global** in the list, and then select **Show Details** on the **Edit** menu.
5. On the **Edit Global Settings** page, select the **Enable call admission control** check box.

### NOTE

If you want to disable call admission control throughout your deployment, clear this check box.

6. Click **Commit**.

## See also

[Get-CsNetworkConfiguration](#)

[Set-CsNetworkConfiguration](#)

[Remove-CsNetworkConfiguration](#)

# Call admission control deployment: final checklist for Skype for Business Server

8/7/2019 • 2 minutes to read

Final checklist for deploying Call Admission Control (CAC) in Skype for Business Server Enterprise Voice.

Use the following checklist to verify that you have completed all the necessary configuration tasks to deploy Call Admission Control (CAC).

- If one or more Edge Servers are deployed, each external interface IP address must be added to the subnet list in the network configuration settings, with a bit mask of 32. You should also associate this subnet (IP address) with the network site ID for the geographic location where the A/V Edge service is deployed.

## NOTE

Edge Servers are not required to implement CAC.

- Make sure that CAC is enabled, as specified in [Enable call admission control in Skype for Business Server](#).
- Make sure that CAC is enabled in all central sites. This can be done through the Topology Builder. If a warning is generated when you publish, *do not* ignore it.
- Make sure that all the subnets that are managed in the enterprise network are configured in the network configuration settings. It is also essential that every subnet be associated to a network site, as explained in [Deploy network regions, sites and subnets in Skype for Business](#).
- Make sure that the subnet or IP addresses of all Front End Servers, Survivable Branch Appliances (SBAs), Audio/Video Conferencing Servers (if in a separate pool), and Mediation Servers are configured in the network configuration settings.



# Deploy emergency services in Skype for Business Server

8/7/2019 • 3 minutes to read

Deploy E9-1-1 in Skype for Business Server Enterprise Voice. Includes prerequisites and deployment process checklist.

Enhanced 9-1-1 (E9-1-1) is an emergency notification feature that associates the calling party's telephone number with a civic or a street address. Using this information, the Public Safety Answering Point (PSAP) can immediately dispatch emergency services to the caller in distress.

To support E9-1-1, Skype for Business Server must be able to correctly associate a location with a client and to make sure that this information is used to route the emergency call to the nearest PSAP.

## Deployment Prerequisites for E9-1-1

Before you deploy E9-1-1, you must already have deployed your Skype for Business Server internal servers, including a Central Management store, a Front End pool or a Standard Edition server. You must also deploy one or more Mediation Servers, either standalone or collocated with Front End Servers. In addition, an E9-1-1 deployment requires a SIP trunk to a qualified E9-1-1 service provider or an Emergency Location Identification Number (ELIN) gateway to your public switched telephone network (PSTN).

## Deployment Process

The following table provides an overview of the E9-1-1 deployment process.

PHASE	STEPS	ROLES	DEPLOYMENT DOCUMENTATION
-------	-------	-------	--------------------------

PHASE	STEPS	ROLES	DEPLOYMENT DOCUMENTATION
<p>Configure voice usages, routes, and trunk configurations</p>	<ol style="list-style-type: none"> <li>1. Create a new PSTN usage record. This is the same name that is used for the <b>PSTN Usage</b> setting in the location policy.</li> <li>2. Create or assign a voice route to the PSTN usage record created in the previous step and then point the gateway attribute to the E9-1-1 SIP trunk or ELIN gateway.</li> <li>3. For a SIP trunk E9-1-1 service provider, set the trunk that will be handling E9-1-1 calls over the SIP to pass PIDF-LO data by using the <b>Set-CsTrunkConfiguration -EnablePIDFLOSupport</b> cmdlet.</li> <li>4. Optionally, for a SIP trunk E9-1-1 service provider, create or assign a local PSTN route for calls that are not handled by the E9-1-1 service provider's SIP trunk. This route will be used if the connection to the E9-1-1 service provider is not available. If supported by your E9-1-1 service provider, assign a trunk configuration rule to the gateway that translates the 911 dial string into the direct inward dialing (DID) number of the national/regional Emergency Call Response Center (ECRC).</li> </ol>	<p>CSVoiceAdmin</p>	<p><a href="#">Configure an E9-1-1 voice route in Skype for Business Server</a></p>
<p>Create location policies and assign them to users and subnets</p>	<ol style="list-style-type: none"> <li>1. Review the global location policy.</li> <li>2. Create a location policy with a user-level scope; or, if the organization has more than one site with different emergency usages, create a location policy with a network-level scope.</li> <li>3. Assign the location policy to network sites.</li> <li>4. Add the appropriate subnets to the network site.</li> <li>5. (Optional) Assign the location policy to user policies.</li> </ol>	<p>CSVoiceAdmin CSLocationAdmin (except for creating Location Policies)</p>	<p><a href="#">Create location policies in Skype for Business Server</a> <a href="#">Add a location policy to a network site in Skype for Business Server</a> <a href="#">Associate a subnet with a network site</a></p>

PHASE	STEPS	ROLES	DEPLOYMENT DOCUMENTATION
Configure the location database	<ol style="list-style-type: none"> <li>1. Populate the database with a mapping of network elements to locations.</li> <li>2. For ELIN gateways, add the ELINs to the &lt;CompanyName&gt; column.</li> <li>3. Configure the connection to the E9-1-1 service provider for validating addresses.</li> <li>4. Validate the addresses with the E9-1-1 service provider.</li> <li>5. Publish the updated database.</li> <li>6. For ELIN gateways, upload the ELINs to your PSTN carrier's Automatic Location Identification (ALI) database.</li> </ol>	CSVoiceAdmin CSLocationAdmin	<a href="#">Configure the location database in Skype for Business Server</a>
Configure Advanced Features (optional)	<ol style="list-style-type: none"> <li>1. Configure the URL for the SNMP application.</li> <li>2. Configure the URL for the location of the Secondary Location Information service.</li> </ol>	CSVoiceAdmin	<a href="#">Configure an SNMP application in Skype for Business Server</a> <a href="#">Configure a secondary Location Information service in Skype for Business Server</a>

# Configure an E9-1-1 voice route in Skype for Business Server

8/7/2019 • 2 minutes to read

Configure E9-1-1 voice routes in Skype for Business Server Enterprise Voice.

To deploy E9-1-1, you first need to configure an emergency call voice route. For details about creating voice routes, see [Create or modify a voice route in Skype for Business](#). You may define more than one route if, for example, your deployment includes a primary SIP trunk and a secondary SIP trunk.

## NOTE

To include location information in an E9-1-1 INVITE, you need to configure the SIP trunk that connects to the E9-1-1 service provider to route emergency calls through the gateway. To do this, set the `EnablePIDFLOSupport` flag on the **Set-CsTrunkConfiguration** cmdlet to True. The default value for `EnablePIDFLOSupport` is False. For example:

```
Set-CsTrunkConfiguration Service:PstnGateway:192.168.0.241 -EnablePIDFLOSupport $true.
```

It is not necessary to enable receiving locations for fallback public switched telephone network (PSTN) gateways and Emergency Location Identification Number (ELIN) gateways.

## To configure an E9-1-1 voice route

1. Log on to the computer with an account that is a member of the `RTCUniversalServerAdmins` groups, or a member of the `CsVoiceAdministrator` administrative role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following cmdlet to create a new PSTN usage record.

This must be the same name that you will use for the **PSTN** setting in the location policy. Although your deployment will have multiple phone usage records, the following example adds "Emergency Usage" to the current list of available PSTN usages. For details, see [Configure voice policies, PSTN usage records, and voice routes in Skype for Business](#).

```
Set-CsPstnUsage -Usage @{add='EmergencyUsage'}
```

4. Run the following cmdlet to create a new voice route by using the PSTN usage record that you created in the previous step.

The number pattern must be the same number pattern that is used in the **Emergency Dial String** setting in the location policy. A "+" sign is needed because Skype for Business adds "+" to emergency calls. "Co1-pstngateway-1" is the SIP trunk service ID for the E9-1-1 service provider or for the ELIN gateway service ID. The following example uses "EmergencyRoute" as the name of the voice route.

```
New-CsVoiceRoute -Name "EmergencyRoute" -NumberPattern "^\\+911$" -PstnUsages @{add="EmergencyUsage"} -PstnGatewayList @{add="co1-pstngateway-1"}
```

5. Optionally, for SIP trunk connections, we recommend that you run the following cmdlet to create a local route for calls that are not handled by the E9-1-1 service provider's SIP trunk. This route will be used if the connection to the E9-1-1 service provider is not available.

The following example assumes that user has "Local" usage in their voice policy.

```
New-CsVoiceRoute -Name "LocalEmergencyRoute" -NumberPattern "^\\+911$" -PstnUsages @{add="Local"} -  
PstnGatewayList @{add="co1-pstngateway-2"}
```

# Create location policies in Skype for Business Server

8/7/2019 • 2 minutes to read

Read this topic to learn how to configure enhanced emergency service (E9-1-1) location policies in Skype for Business Server Enterprise Voice.

Skype for Business Server uses a location policy to enable Skype for Business clients for E9-1-1 during client registration. A location policy contains the settings that define how E9-1-1 will be implemented. For more information, see [Plan location policies for Skype for Business Server](#).

You define location policies by using the Skype for Business Control Panel or by using the [New-CsLocationPolicy](#) cmdlet.

## NOTE

Skype for Business Server now supports the configuration of multiple emergency numbers for a client. If you want to configure multiple emergency numbers, you must follow the information in [Plan for multiple emergency numbers in Skype for Business Server](#) and [Configure multiple emergency numbers in Skype for Business](#).

You can edit the global location policy and create new tagged location policies. A client obtains a global policy when it is not located within a subnet with an associated location policy, or when the client has not been directly assigned a location policy. Tagged policies are assigned to subnets or users.

To create a location policy, you must use an account that is a member of the RTCUniversalServerAdmins group, or is a member of the CsVoiceAdministrator administrative role, or has equivalent administrator rights and permissions.

For more information, see [Plan location policies for Skype for Business Server](#). Cmdlets in this procedure use a location policy defined using the following values. For a complete description of cmdlet parameters and values, see [New-CsLocationPolicy](#).

ELEMENT	VALUE
EnhancedEmergencyServicesEnabled	<b>True</b>
LocationRequired	<b>Disclaimer</b>
EnhancedEmergencyServiceDisclaimer	Your company policy requires you to set a location. If you do not set a location, emergency services will not be able to locate you in an emergency. Please set a location.
UseLocationForE911Only	<b>False</b>
PstnUsage	<b>EmergencyUsage</b>
EmergencyDialString	<b>911</b>
EmergencyDialMask	<b>112</b>
NotificationUri	<b>sip:security@litwareinc.com</b>

ELEMENT	VALUE
ConferenceUri	<b>sip: +14255550123@litwareinc.com</b>
ConferenceMode	<b>twoway</b>
LocationRefreshInterval	<b>2</b>

### To create location policies

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.

#### NOTE

CsLocationPolicy will fail if the setting for **PstnUsage** is not already in the Global list of PstnUsages.

2. Optionally, run the following cmdlet to edit the global Location Policy:

```
Set-CsLocationPolicy -Identity Global -EnhancedEmergencyServicesEnabled $true -LocationRequired "disclaimer" -EnhancedEmergencyServiceDisclaimer "Your company policy requires you to set a location. If you do not set a location emergency services will not be able to locate you in an emergency. Please set a location." -PstnUsage "emergencyUsage" -EmergencyDialString "911" -ConferenceMode "twoway" -ConferenceUri "sip:+14255550123@litwareinc.com" -EmergencyDialMask "112" NotificationUri "sip:security@litwareinc.com" -UseLocationForE911Only $true -LocationRefreshInterval 2
```

3. Run the following to create a tagged Location Policy.

```
New-CsLocationPolicy -Identity Tag:Redmond - EnhancedEmergencyServicesEnabled $true -LocationRequired "disclaimer" -EnhancedEmergencyServiceDisclaimer "Your company policy requires you to set a location. If you do not set a location emergency services will not be able to locate you in an emergency. Please set a location." -UseLocationForE911Only $false -PstnUsage "EmergencyUsage" -EmergencyDialString "911" -EmergencyDialMask "112" -NotificationUri "sip:security@litwareinc.com" -ConferenceUri "sip:+14255550123@litwareinc.com" -ConferenceMode "twoway" -LocationRefreshInterval 2
```

4. Run the following cmdlet to apply the tagged Location Policy created in step 3 to a user policy.

```
(Get-CsUser | where { $_.Name -match "UserName" }) | Grant-CsLocationPolicy -PolicyName Redmond
```

# Add a location policy to a network site in Skype for Business Server

8/7/2019 • 2 minutes to read

Assign E9-1-1 location policies to network sites in Skype for Business Server Enterprise Voice.

The following examples show how to add the **Redmond** location policy defined in [Create location policies in Skype for Business Server](#) to an existing network site and how to create a new network site that uses the **Redmond** location policy.

For details about working with network sites, see the Lync Server Management Shell documentation for the following cmdlets:

- **New-CsNetworkSite**
- **Get-CsNetworkSite**
- **Set-CsNetworkSite**
- **Remove-CsNetworkSite**

## To assign a location policy to an existing network site

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the following cmdlets to modify an existing network site.

Assign the **Redmond** tagged Location policy to an existing network site named **Redmond**.

```
Set-CsNetworkSite -Identity "Redmond" -NetworkRegionID "NorthAmerica" -LocationPolicy "Redmond"
```

## To assign a location policy to a new network site

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the following cmdlet to create a new network site.

Create a new network site in the network region and assign the **Redmond** tagged Location policy.

```
New-CsNetworkSite -Identity "Redmond" -NetworkRegionID "NorthAmerica" -LocationPolicy "Redmond"
```



# Configure the location database in Skype for Business Server

11/7/2019 • 4 minutes to read

Configure, populate, and publish the E9-1-1 location database in Skype for Business Server Enterprise Voice.

To enable clients to automatically detect their location within a network, you first need to configure the location database.

To configure the location database, perform the following tasks:

- Populate the database with a mapping of network elements to locations. If you use an Emergency Location Identification Number (ELIN) gateway, you need to include the ELIN in the <CompanyName> field.

If you do not populate the location database, and the **Location Required** in the Location Policy is set to **Yes** or **Disclaimer**, the client will prompt the user to enter a location manually.

- Validate the addresses against the master street address guide (MSAG) that is maintained by the E9-1-1 service provider.
- Publish the updated database.

## Populate the location database

To automatically locate clients within a network, you first need to populate the location database with a network wiremap, which maps network elements to civic (that is, street) addresses. You can use subnets, wireless access points, switches, and ports to define the wiremap.

You can add addresses to the location database individually, or in bulk by using a CSV file that contains the column formats described in the following table.

If you use an Emergency Location Identification Number (ELIN) gateway, include the ELIN in the **CompanyName** field for each location. You can include multiple ELINs for each location, each separated by a semicolon.

NETWORK ELEMENT	REQUIRED COLUMNS
<b>Wireless access point</b>	<BSSID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
<b>Subnet</b>	<Subnet>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
<b>Port</b>	<ChassisID>,<PortIDSubType>,<PortID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,...<PreDirectional>,<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>

NETWORK ELEMENT	REQUIRED COLUMNS
Switch	<ChassisID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>

## To add network elements to the location database

1. Run the following cmdlet to add a subnet location to the location database.

```
Set-CsLisSubnet -Subnet 157.56.66.0 -Description "Subnet 1" -Location Location1 -CompanyName "Litware" -HouseNumber 1234 -HouseNumberSuffix "" -PreDirectional "" -StreetName 163rd -StreetSuffix Ave -PostDirectional NE -City Redmond -State WA -PostalCode 99123 -Country US
```

For ELIN gateways, put the ELIN in the CompanyName field. You can include more than one ELIN. For example:

```
Set-CsLisSubnet -Subnet 157.56.66.0 -Description "Subnet 1" -Location Location1 -CompanyName 425-555-0100; 425-555-0200; 425-555-0300 -HouseNumber 1234 -HouseNumberSuffix "" -PreDirectional "" -StreetName 163rd -StreetSuffix Ave -PostDirectional NE -City Redmond -State WA -PostalCode 99123 -Country US
```

Alternately, you can run the following cmdlets and use a file named "subnets.csv" to bulk update subnet locations.

```
$g = Import-Csv subnets.csv
$g | Set-CsLisSubnet
```

2. Run the following cmdlet to add wireless locations to the location database.

```
Set-CsLisWirelessAccessPoint -BSSID 0A-23-CD-16-AA-2E -Description "Wireless1" -Location Location2 -CompanyName "Litware" -HouseNumber 2345 -HouseNumberSuffix "" -PreDirectional "" -StreetName 163rd -StreetSuffix Ave -PostDirectional NE -City Bellevue -State WA -PostalCode 99234 -Country US
```

Alternately, you can run the following cmdlets and use a file named "waps.csv" to bulk update wireless locations.

```
$g = Import-Csv waps.csv
$g | Set-CsLisWirelessAccessPoint
```

3. Run the following cmdlet to add switch locations to the location database.

```
Set-CsLisSwitch -ChassisID 0B-23-CD-16-AA-BB -Description "Switch1" -Location Location1 -CompanyName "Litware" -HouseNumber 1234 -HouseNumberSuffix "" -PreDirectional "" -StreetName 163rd -StreetSuffix Ave -PostDirectional NE -City Redmond -State WA -PostalCode 99123 -Country US
```

Alternately, you can run the following cmdlets and use a file named "switches.csv" to bulk update switch locations.

```
$g = Import-Csv switches.csv
$g | Set-CsLisSwitch
```

4. Run the following cmdlet to add port locations to the location database

```
Set-CsLisPort -ChassisID 0C-23-CD-16-AA-CC -PortID 0A-abcd -Description "Port1" -Location Location2 -
CompanyName "Litware" -HouseNumber 2345 -HouseNumberSuffix "" -PreDirectional "" -StreetName 163rd -
StreetSuffix Ave -PostDirectional NE -City Bellevue -State WA -PostalCode 99234 -Country US
```

The default for PortIDSubType is LocallyAssigned. You can also set it to InterfaceAlias or InterfaceName

Alternately, you can run the following cmdlets and use a file named "ports.csv" to bulk update port locations.

```
$g = Import-Csv ports.csv
$g | Set-CsLisPort
```

## Validate addresses

### To validate addresses located in the location database

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the following cmdlets to configure the emergency service provider connection.

```
$pwd = Read-Host -AsSecureString <password>
Set-CsLisServiceProvider -ServiceProviderName Provider1 -ValidationServiceUrl <URL provided by provider>
-CertFileName <location of certificate provided by provider> -Password $pwd
```

3. Run the following cmdlet to validate the addresses in the location database.

```
Get-CsLisCivicAddress | Test-CsLisCivicAddress -UpdateValidationStatus
```

You can also use the **Test-CsLisCivicAddress** cmdlet to validate individual addresses.

## Publish the location database

The new locations that you added to the location database will not be made available to the client until they have been published.

If you use Emergency Location Identification Number (ELIN) gateways, you also need to upload the ELINs to your public switched telephone network (PSTN) carrier's Automatic Location Identification (ALI) database. Your PSTN carrier may require you to use a specific format for the ELIN records. Contact your PSTN carrier for details. You can export the records from the Location Information service database and format them as required.

### To publish the location database

- Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
- Run the following cmdlet to publish the location database.

```
Publish-CsLisConfiguration
```

# Configure an SNMP application in Skype for Business Server

8/7/2019 • 2 minutes to read

Configure an SNMP application to work with E9-1-1 in Skype for Business Server Enterprise Voice.

Skype for Business Server includes a standard web service interface that you can use to connect the Location Information service to Simple Network Management Protocol (SNMP) applications that match MAC addresses with port and switch information.

If an SNMP application is installed and the Location Information service fails to find a match in the location database, the Location Information service automatically queries the application by using the MAC address provided by the client. The Location Information service then uses the port and switch information returned by the SNMP application to query the location database again.

## NOTE

MAC addresses are not available on computers running Windows 8.

## To configure the SNMP application URL

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the following cmdlet to configure the URL for the SNMP application.

```
Set-CsWebServiceConfiguration -MACResolverUrl "<SNMP application url>"
```

## See also

[Set-CsWebServiceConfiguration](#)

# Configure a secondary Location Information service in Skype for Business Server

8/7/2019 • 2 minutes to read

Configure a secondary location source (SLS) database for E9-1-1 in Skype for Business Server Enterprise Voice.

Skype for Business Server provides a web service interface that you can use to point the Location Information service to a Secondary Location Source (SLS) database. The web service interface that connects to the SLS database must conform to Location Information service WSDL. If both a location database and secondary location database are configured, the Location Information service first queries the location database, and if no match is found, sends the location request from the client to the SLS database. If the location exists in the SLS, the Location Information service then sends the location back to the client.

## To configure a Secondary Location database

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run the following cmdlet to configure the URL for the location of the secondary location database.

```
Set-CsWebServiceConfiguration -SecondaryLocationSourceURL "<web service url>"
```

## See also

[Set-CsWebServiceConfiguration](#)

# Configure multiple emergency numbers in Skype for Business

8/7/2019 • 2 minutes to read

Read this topic to learn how to configure multiple emergency numbers in Skype for Business Server.

Skype for Business Server now supports multiple emergency numbers for a client. Multiple emergency numbers is a new feature introduced in the June 2016 Cumulative Update. Before you configure your environment to support multiple emergency numbers, be sure to read [Plan for multiple emergency numbers in Skype for Business Server](#).

## NOTE

If you have not yet upgraded to the November 2016 Cumulative Update, see [Updates to Skype for Business Server 2015](#). With the November 2016 Cumulative Update, the number of support emergency numbers increases from 5 to 100.

## Configure multiple emergency numbers

To configure multiple emergency numbers, you use the `New-CsEmergencyNumber` cmdlet, and then you specify the `EmergencyNumbers` parameter with the [New-CsLocationPolicy](#) and [Set-CsLocationPolicy](#) cmdlets. For a complete description of all the location policy parameters, such as PSTN usage and Location required, see [Set-CsLocationPolicy](#).

The following command creates a new emergency number with dial string 911 by using the `New-CsEmergencyNumber` cmdlet:

```
> $a = New-CsEmergencyNumber -DialString 911
```

The next command associates the number with the specified location policy by specifying the `EmergencyNumbers` parameter in the `Set-CsLocationPolicy` cmdlet:

```
> Set-CsLocationPolicy -Identity <id> -EmergencyNumbers @{add=$a}
```

In the next example, an emergency number is created with a single dial mask, 112:

```
> $a = New-CsEmergencyNumber -DialString 911 -DialMask 112
```

The next command creates an emergency number with multiple dial masks:

```
> $a = New-CsEmergencyNumber -DialString 911 -DialMask 112;999
```

The next example adds multiple emergency numbers with multiple dial masks, and then associates the emergency numbers with the specified location policy:

```
> $a = New-CsEmergencyNumber -DialString 911 -DialMask 112;999
> $b = New-CsEmergencyNumber -DialString 500 -DialMask 501;502
> Set-CsLocationPolicy -Identity <id> -EmergencyNumbers @{add=$a,$b}
```

The next example configures multiple emergency numbers for health care providers that use both 911 and 450:

```
> $a = New-CsEmergencyNumber -DialString 911
> $b = New-CsEmergencyNumber -DialString 450
> Set-CsLocationPolicy -Identity US-Hospital -EmergencyNumbers @{add=$a,$b}
```

The next example configures multiple emergency numbers for the city of London:

```
> $a = New-CsEmergencyNumber -DialString 999 -DialMask 144
> $b = New-CsEmergencyNumber -DialString 112 -DialMask 911;117;118
> Set-CsLocationPolicy -Identity London -EmergencyNumbers @{add=$a,$b}
```

The next example configures multiple emergency numbers for India:

```
> $a = New-CsEmergencyNumber -DialString 100 -DialMask 911
> $b = New-CsEmergencyNumber -DialString 101
> $c = New-CsEmergencyNumber -DialString 102
> Set-CsLocationPolicy -Identity India -EmergencyNumbers @{add=$a,$b,$c}
```

The next example removes an existing entry with Dial string 911 and Dial masks 112 and 999:

```
> $a = New-CsEmergencyNumber -DialString 911 -DialMask 112;999
> Set-CsLocationPolicy -Identity <id> -EmergencyNumbers @{remove=$a}
```

# Deploy media bypass in Skype for Business Server

8/7/2019 • 4 minutes to read

Deploy media bypass in Skype for Business Server Enterprise Voice. Includes prerequisites and deployment process checklist.

This topic assumes that you have already published and configured either at least one or more Mediation Servers and at least one gateway peer to provide PSTN connectivity. For more details on those tasks, see [Deploy a Mediation Server in Topology Builder in Skype for Business Server](#) and [Define a gateway in Topology Builder in Skype for Business Server](#).

If the peer you connect to is the SBC of a SIP trunking provider, make sure that the provider is a qualified provider and that the provider supports media bypass. For example, many SIP trunking providers will only allow their SBC to receive traffic from the Mediation Server. If so, then bypass must not be enabled for the trunk in question. Also, you cannot enable media bypass unless your organization reveals its internal network IP addresses to the SIP trunking provider.

## NOTE

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on [Unified Communications Open Interoperability Program - Lync Server](#).

If you have already optionally configured call admission control (CAC), another advanced Enterprise Voice feature, note that the bandwidth reservation performed by call admission control does not apply to any calls for which media bypass is employed. The verification of whether to employ media bypass is performed first, and if media bypass is employed, call admission control is not used for the call; only if the media bypass check fails is the check performed for call admission control. The two features are thus mutually exclusive for any particular call that is routed to the PSTN. This is the logic because media bypass assumes that bandwidth constraints do not exist between the media endpoints on a call; media bypass cannot be performed on links with restricted bandwidth. As a result, one of the following will apply to a PSTN call: a) media bypasses the Mediation Server, and call admission control does not reserve bandwidth for the call; or b) call admission control applies bandwidth reservation to the call, and media is processed by the Mediation Server involved in the call.

In addition to enabling media bypass for individual trunk connections associated with a peer, you must also enable media bypass globally. Global media bypass settings can either specify that media bypass is always attempted for calls to the PSTN, or that media bypass is employed by using the mapping of subnets to network sites and network regions—similar to what is done by call admission control, another advanced voice feature. When media bypass and call admission control are both enabled, then the network region, network site, and subnet information that is specified for call admission control is automatically used when determining whether to employ media bypass. This means that you cannot specify that media bypass is always attempted for calls to the PSTN when call admission control is enabled.



**NOTE**

When you use these steps to configure media bypass, the assumption is that you have good connectivity between clients and the Mediation Server peer (for example, a PSTN gateway, an IP-PBX, or an SBC at a SIP trunking provider). If there are any bandwidth limitations on the link, media bypass cannot be applied to the call. Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on [Unified Communications Open Interoperability Program - Lync Server](#).

## Deployment Process for media bypass

The following table provides an overview of the media bypass deployment process.

PHASE	STEPS	ROLES	DEPLOYMENT DOCUMENTATION
Configure trunks for media bypass	If you have not already done so, configure one or more trunks for media bypass.	A member of RTCUniversalServerAdmins group, or a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role	<a href="#">Configure a trunk with media bypass in Skype for Business Server</a>
Configure media bypass globally	Configure media bypass for either all calls to the PSTN, or certain calls based on network sites and network regions.	A member of RTCUniversalServerAdmins group, or a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role	<a href="#">Configure media bypass in Skype for Business Server to always bypass the Mediation Server</a> <a href="#">Configure media bypass global settings in Skype for Business Server to use site and region information</a>
Associate subnets with network sites, if necessary	If you configure media bypass to use site and region information, you must associate the subnets of your deployment with network sites and regions (If you have not already done so for another voice feature.)	A member of RTCUniversalServerAdmins group, or a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role	<a href="#">Associate a subnet with a network site</a>

# Configure media bypass in Skype for Business Server to always bypass the Mediation Server

8/7/2019 • 2 minutes to read

Enable media bypass to always bypass the Mediation Server in Skype for Business Server Enterprise Voice.

If you use the steps in this topic to configure global settings for media bypass, the assumption is that you have good connectivity between Skype for Business endpoints and any peer for which you configured media bypass on the trunk connection.

If you do not have good connectivity between Skype for Business endpoints and all peers to the Mediation Server whose respective trunk connections have been enabled for media bypass, you must configure global media bypass settings to use site and region information when employing media bypass. This allows for more control in determining when media bypasses the Mediation Server. To do this, use the steps in [Configure media bypass global settings in Skype for Business Server to use site and region information](#) and [Associate a subnet with a network site](#) instead.

## To Enable Media Bypass Globally to Always Bypass the Mediation Server

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Double-click the **Global** configuration in the list.
4. On the **Edit Global Setting** page, select the **Enable media bypass** check box.
5. Click **Always bypass**.
6. Click **Commit**.

## See also

[Plan for media bypass in Skype for Business](#)

[Deploy media bypass in Skype for Business Server](#)

# Configure media bypass global settings in Skype for Business Server to use site and region information

8/7/2019 • 2 minutes to read

Configure media bypass to be used for only certain sites and regions in Skype for Business Server Enterprise Voice.

If you use the steps in this topic to configure global settings for media bypass, the assumption is that you do not have good connectivity between all Skype for Business endpoints and any peer for which you configured media bypass on the trunk connection.

## NOTE

Network region and network site information is shared between call admission control and media bypass advanced Enterprise Voice features when both are enabled. Therefore, if you have already configured call admission control, you are not required to use the following procedure to edit the site and region information specifically for media bypass. Follow the steps in this procedure if you have not yet configured network regions and sites for call admission control, and you want to change media bypass settings.

For media bypass to work properly there must be consistency between a site as defined in Topology Builder and as it is defined when you configure network regions and network sites. For example, if you have a branch site that you defined in Topology Builder as having only a PSTN gateway deployed, then that branch site must be configured with an Enterprise Voice policy that enables branch site users to have their PSTN calls routed through the PSTN gateway at the branch site.

## To Configure Site and Region Information for Media Bypass

1. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
2. In the left navigation bar, click **Network Configuration**.
3. Double-click the **Global** configuration in the table.
4. On the **Edit Global Setting** page, select the **Enable media bypass** check box.
5. Click **Use sites and region configuration**.
6. If necessary, select the **Enable bypass for non-mapped sites** check box.

## NOTE

Select this check box only if you have one or more large sites associated with the same region that do not have bandwidth constraints (for example, a large central site), but you also have some branch sites associated with the same region that do have bandwidth constraints. When you enable bypass for non-mapped sites, configuration is streamlined in that you specify only the subnets associated with the branch sites, rather than needing to specify all subnets associated with all sites. We recommend that you do not select this check box if call admission control is enabled.

7. Click **Commit**.

Next, add subnets to the network site, as described in [Associate a subnet with a network site](#). After you associate

all subnets with network sites, media bypass deployment is complete.

**IMPORTANT**

If you have not already created network regions and network sites, you must first create those before you can proceed with media bypass deployment. For details, see [Deploy network regions, sites and subnets in Skype for Business](#).

## See also

[Associate a subnet with a network site](#)

# Deploy call management features in Skype for Business

8/7/2019 • 2 minutes to read

Deploying call management features in Skype for Business Server Enterprise Voice.

Enterprise Voice call management features control how incoming calls are routed and answered. Skype for Business Server provides the following call management features:

- **Call Park:** Enables voice users to temporarily park a call and then pick it up from the same phone or another phone.
- **Group Call Pickup:** Enables users to answer calls made to another user who is assigned to a pickup group by dialing the call pickup group number.
- **Response Group:** Routes incoming calls to groups of agents by using hunt groups or interactive voice response (IVR) questions and answers.
- **Announcement:** Plays a message for calls made to an unassigned number, or routes the call elsewhere, or both.

This section describes how to configure these call management features during an Enterprise Voice deployment.

## In this section

- [Deployment process for Call Park in Skype for Business](#)
- [Deployment process for Group Call Pickup in Skype for Business](#)
- [Deployment process for Response Group in Skype for Business](#)
- [Deployment process for the Announcement application in Skype for Business Server](#)

# Deployment process for Call Park in Skype for Business

8/7/2019 • 2 minutes to read

Deployment process and steps for call park in Skype for Business Server Enterprise Voice.

Call Park enables an Enterprise Voice user to put a call on hold from one telephone and then retrieve the call later by dialing an internal number (known as a Call Park orbit) from any telephone.

The components that Call Park uses are automatically installed and enabled on the Front End Server or Standard Edition server when you deploy Enterprise Voice. However, you must use the following steps to configure Call Park before it is available to users.

## Call Park Deployment Process

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Configure the call park orbit ranges in the orbit table	<p>Use Skype for Business Server Control Panel or the <b>New-CSCallParkOrbit</b> cmdlet to create the orbit ranges in the call park orbit table and associate them with the Application service that hosts the Call Park application.</p> <p><b>Note:</b> For seamless integration with existing dial plans, orbit ranges are typically configured as a block of virtual extensions. Assigning Direct Inward Dialing (DID) numbers as orbit numbers in the call park orbit table is not supported.</p>	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	<a href="#">Create or modify a Call Park orbit range in Skype for Business</a>

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Configure Call Park settings	<p>Use the <b>Set-CsCpsConfiguration</b> cmdlet to configure Call Park settings. At a minimum, we recommend that you configure the <b>OnTimeoutURI</b> option to configure the fallback destination to use when a parked call times out. You can also configure the following settings:</p> <p>(Optional)  <b>EnableMusicOnHold</b> to enable or disable music on hold.</p> <p>(Optional)  <b>MaxCallPickupAttempts</b> to determine the number of times a parked call rings back to the answering phone before forwarding the call to the fallback Uniform Resource Identifier (URI).</p> <p>(Optional)  <b>CallPickupTimeoutThreshold</b> to determine the amount of time that elapses after a call has been parked before it rings back to the phone where the call was answered.</p>	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	<a href="#">Configure Call Park settings in Skype for Business</a>
Optionally, customize the music on hold	<p>Use the <b>Set-CsCallParkServiceMusicOnHoldFile</b> cmdlet to customize and upload an audio file, if you don't want to use the default music on hold.</p>	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	<a href="#">Customize Call Park music on hold in Skype for Business</a>
Configure voice policy to enable Call Park for users	<p>Use Skype for Business Server Control Panel or the <b>Set-CsVoicePolicy</b> cmdlet with the <b>EnableCallPark</b> option to enable Call Park for users in voice policy. By default, Call Park is disabled for all users. If you have multiple voice policies, make sure the <b>EnableCallPark</b> property is set for each voice policy, not just for the default policy.</p>	RTCUniversalServerAdmins CsVoiceAdministrator CsUserAdministrator CsAdministrator	<a href="#">Enable Call Park for users in Skype for Business</a>

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Verify normalization rules for Call Park	Call park orbits must not be normalized. Verify that your normalization rules do not include any of your orbit ranges. If necessary, create additional normalization rules to prevent orbits being normalized.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	<a href="#">Verify normalization rules for Call Park in Skype for Business</a>
Verify your Call Park deployment	Test parking and retrieving calls to make sure that your configuration works as expected.	-	<a href="#">(Optional) Verify Call Park deployment in Skype for Business</a>



# Create or modify a Call Park orbit range in Skype for Business

8/7/2019 • 4 minutes to read

Create or modify a Call Park orbit range table in Skype for Business Server Enterprise Voice.

Call Park uses orbits for parking calls. Before users can park and retrieve calls, you must configure the Call Park orbit table. You need to specify the ranges of extension numbers (orbits) that your organization will reserve for parking calls and define the routing for those ranges by specifying which Call Park pool handles each range. When you define orbit ranges, the goal is to have enough orbits so that any one orbit is not reused too quickly, but not so many orbits that you limit the number of extensions available for users or other services. You can create multiple Call Park orbit ranges for each Skype for Business Server pool where the Call Park application is deployed. Each Call Park orbit range must have a globally unique name and a unique set of extensions.

## IMPORTANT

An orbit range typically encompasses 100 or fewer orbits. Each range can be much larger, as long as it is smaller than the maximum of 10,000 orbits per range and you have fewer than 50,000 orbits per pool. If a range is too small, the orbits are reused more quickly.

Use blocks of virtual extensions (extensions that have no user or phone assigned to them) for your orbit ranges.

## NOTE

Assigning Direct Inward Dialing (DID) numbers as orbit numbers in the Call Park orbit table is not supported.

Use one of the following procedures to create or modify a call park orbit range.

### To use Skype for Business Server Control Panel to create or modify a range of numbers for parking calls

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Features** and then click **Call Park**.
4. On the **Call Park** page, do one of the following:
  - To create a new orbit range, click **New**. In **Name**, type an identifying name for this range of numbers.

## NOTE

After you commit the orbit range to the database, you cannot change this name.

- To modify an existing orbit range, type all or part of the name of the orbit range in the search field. In the resulting list of orbits, click the orbit you want, click **Edit**, and then click **Show details**.
5. In the first **Number range** field, type the beginning number of the range of extensions for this call park

orbit, and in the second **Number range** field, type the ending number of the range. Be aware:

- The beginning number of the range must be less than or equal to the ending number of the range.
- The value of the beginning number of the range must be the same length as the ending number of the range.
- The orbit range must be unique. This range cannot overlap with any other range.
- If the orbit range begins with the character \* or #, the range must be greater than 100.
- Valid values: Must match the regular expression string `([*|#]?[1-9]\d{0,7})|([1-9]\d{0,8})`. This means the value must be a string beginning with either the character \* or # or a number 1 through 9 (the first character cannot be a zero). If the first character is \* or #, the following character must be a number 1 through 9 (it cannot be a zero). Subsequent characters can be any number 0 through 9 up to seven additional characters (for example, "#6000", "\*92000", "\*95551212", and "915551212"). If the first character is not \* or #, the first character must be a number 1 through 9 (it cannot be zero), followed by up to eight characters, each a number 0 through 9 (for example, "915551212", "41212", "300").
- You should not have more than a total of 50,000 orbits per pool. Each orbit range typically encompasses 100 or fewer orbits, but it can be much larger as long as it includes fewer than 10,000 orbits. For example, instead of specifying a starting number of "7000000" and an ending number of "8000000," consider specifying a starting number of "7000000" and an ending number of "7000100."

6. In **FQDN of destination server**, click the fully qualified domain name (FQDN) or service ID of the Application service that hosts the Call Park application. All calls parked to numbers within the range specified by the start number and end number in the orbit range will be routed to this server or pool.

7. Click **Commit**.

### To use Skype for Business Server Management Shell to create or modify a range of numbers for parking calls

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Use **New-CsCallParkOrbit** to create a new range of orbit numbers. Use **Set-CsCallParkOrbit** to modify an existing range of orbit numbers.

At the command line, run:

```
New-CsCallParkOrbit -Identity <name of orbit range> -NumberRangeStart <first number in orbit range> -NumberRangeEnd <last number in orbit range> -CallParkService <FQDN or service ID of the Application service that hosts the Call Park application>
```

For example:

```
New-CsCallParkOrbit -Identity "Redmond orbit 1" -NumberRangeStart 100 -NumberRangeEnd 199 -CallParkService redmond-applicationserver-1
```

The following example shows how to modify the numbers in an existing orbit range,

```
Set-CsCallParkOrbit -Identity "Redmond orbit 1" -NumberRangeStart 500 -NumberRangeEnd 699
```

## See also

[New-CsCallParkOrbit](#)

[Set-CsCallParkOrbit](#)

[Delete a Call Park Orbit Range](#)

# Configure Call Park settings in Skype for Business

8/7/2019 • 2 minutes to read

Modify Call Park settings in Skype for Business Server Enterprise Voice.

If you don't want to use default Call Park settings, you can customize them. When you install the Call Park application, global settings are configured by default. You can modify the global settings, and you can also specify site-specific settings. Use the **New-CsCpsConfiguration** cmdlet to create new site-specific settings. Use the **Set-CsCpsConfiguration** cmdlet to modify existing settings.

## NOTE

At a minimum, we recommend that you configure the **OnTimeoutURI** option for the fallback destination to use when a parked call times out and ringback fails.

Use **New-CsCpsConfiguration** cmdlet or the **Set-CsCpsConfiguration** cmdlet to configure any of the following settings:

THIS OPTION:	SPECIFIES THIS:
<b>CallPickupTimeoutThreshold</b>	The amount of time that elapses after a call has been parked before it rings back to the phone where the call was answered. The value must be entered in the format hh:mm:ss to specify the hours, minutes, and seconds. The minimum value is 10 seconds, and the maximum value is 10 minutes. The default is 00:01:30.
<b>EnableMusicOnHold</b>	Whether music plays for a caller while a call is parked. Values are True or False. The default is True.
<b>MaxCallPickupAttempts</b>	The number of times a parked call rings back to the answering phone before it is forwarded to the fallback Uniform Resource Identifier (URI) that is specified for <b>OnTimeoutURI</b> . The default is 1.
<b>OnTimeoutURI</b>	The SIP address of the user or response group to which an unanswered parked call is routed when <b>MaxCallPickupAttempts</b> is exceeded. Value must be a SIP URI beginning with the string sip:. For example, sip:bob@contoso.com. The default is no forwarding address.

## To configure Call Park settings

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
2. Run:

```
New-CsCpsConfiguration -Identity site:<sitename to apply settings> [-CallPickupTimeoutThreshold <hh:mm:ss>] [-EnableMusicOnHold <$true | $false>] [-MaxCallPickupAttempts <number of rings>] [-OnTimeoutURI sip:<sip URI for routing unanswered call>]
```

**TIP**

Use the **Get-CsSite** cmdlet to identify the site. For details, see [Skype for Business Server Management Shell documentation](#).

For example:

```
New-CsCpsConfiguration -Identity site:Redmond1 -CallPickupTimeoutThreshold 00:01:00 -EnableMusicOnHold $false -MaxCallPickupAttempts 2 -OnTimeoutURI sip:bob@contoso.com
```

## See also

[Customize Call Park music on hold in Skype for Business 2015](#)

[New-CsCpsConfiguration](#)

[Set-CsCpsConfiguration](#)

[Get-CsSite](#)

# Customize Call Park music on hold in Skype for Business

8/7/2019 • 2 minutes to read

Customize the Call Park music on hold in Skype for Business Server Enterprise Voice.

You can specify your own music file to use for music on hold, instead of the default music file that ships with Skype for Business Server. To customize music on hold, use the **Set-CsCallParkServiceMusicOnHoldFile** cmdlet.

## NOTE

If you customize music on hold and want the same music for multiple sites, you must configure the music file for each site that runs the Call Park application.

## To customize the music file

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run:

```
Set-CsCallParkServiceMusicOnHoldFile -Service <ServiceID where the Call Park application resides> -Content <Byte >
```

## TIP

Use the **Get-CsService** cmdlet to identify the service. For details, see [Get-CsService](#).

The following example shows how to obtain the contents of a file, soothingmusic.wma, as a byte array and assign it to a variable. Then the audio file is assigned as the music-on-hold file for Call Park. For details, see [Set-CsCallParkServiceMusicOnHoldFile](#).

```
$a = Get-Content -ReadCount 0 -Encoding byte "C:\MoHFiles\soothingmusic.wma"  
Set-CsCallParkServiceMusicOnHoldFile -Service Redmond1-applicationserver-1 -Content $a
```

## See also

[Set-CsCallParkServiceMusicOnHoldFile](#)

[Get-CsService](#)

# Enable Call Park for users in Skype for Business

8/7/2019 • 2 minutes to read

Enable users for Call Park in Skype for Business Server Enterprise Voice.

By default, Call Park is disabled for all users. Users cannot park calls or retrieve parked calls until they are enabled for Call Park in voice policy.

You can enable Call Park at the global scope, or at the site scope or user scope. User scope takes precedence over site scope, and site scope takes precedence over global scope. If you have multiple voice policies, review all the policies to enable Call Park, not just the global policy.

## To Use Skype for Business Server Control Panel to Enable Call Park for Users

1. Log on to the computer as a member of the **RTCUniversalServerAdmins** group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Routing**.
4. Click the **Voice Policy** tab.
5. Double-click an existing voice policy to open the **Edit Voice Policy** dialog box.
6. Under **Calling features**, select **Enable call park**.
7. Click **OK** to save the voice policy

## To Use Cmdlets to Enable Call Park for Users

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator administrative role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run:

```
Set-CsVoicePolicy -Identity <VoicePolicy> -EnableCallPark $true
```

For example, to enable Call Park for the default global voice policy:

```
Set-CsVoicePolicy -EnableCallPark $true
```

## See also

[Create or modify a voice policy and configure PSTN usage records in Skype for Business](#)

# Verify normalization rules for Call Park in Skype for Business

8/7/2019 • 2 minutes to read

Learn about normalization rules for Call Park in Skype for Business Server Enterprise Voice.

Call Park orbits must not be normalized. Check your dial plans to be sure that your orbit numbers are not normalized. If you must create an additional normalization rule to prevent your orbits from being normalized, follow the procedure in [Create or modify a dial plan in Skype for Business Server](#) to define a new normalization rule, so that **Pattern to match** identifies the orbit range and **Translation pattern** is **\$1**. For example, if your Call Park orbit range is 7000 - 7999, the **Pattern to match** is **^(7\d{3})\$** and **Translation pattern** is **\$1**.

## IMPORTANT

Be sure that the default normalization rule in your dial plans does not contain **^(d\*)**. Otherwise, your Call Park normalization rule will never run.

## See also

[Create or modify a dial plan in Skype for Business Server](#)



# (Optional) Verify Call Park deployment in Skype for Business

8/7/2019 • 2 minutes to read

Verifying your deployment of Call Park in Skype for Business Server Enterprise Voice.

After you install and configure Call Park, you need to verify the configuration to make sure that parking and retrieving calls works as expected. At minimum, verify the following:

- Call a user who has Call Park enabled and have the user park the call.

## NOTE

If you enabled Call Park in voice policy just before performing this test, the user who is parking the call needs to sign out of Skype for Business, and then sign back in, to be able to see the Call Park option in the transfer call list.

- Dial the orbit number to retrieve the call.
- Park another call, let the parked call time out, and do not pick up the ringback. Verify that the timed-out call is correctly routed to the fallback destination that is specified for **OnTimeoutURI**.

# Deployment process for Group Call Pickup in Skype for Business

8/7/2019 • 2 minutes to read

Deployment process and steps for Group Call Pickup in Skype for Business Server Enterprise Voice.

Group Call Pickup enables users to answer incoming calls to their colleagues from their own phones.

The components that Group Call Pickup uses are automatically installed and enabled on the Front End Server or Standard Edition server when you deploy Enterprise Voice. However, you must use the following steps to configure Group Call Pickup before it is available to users.

## Group Call Pickup Deployment Process

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Enable the SEFAUtil tool in your topology	Use the New-CsTrustedApplicationPool cmdlet to create a new trusted application pool. Use the New-CsTrustedApplication cmdlet to specify the SEFAUtil tool as trusted application. Run the Enable-CsTopology cmdlet to enable the topology. If you don't already have it, download the Skype for Business Server version of the SEFAUtil tool from this location, and install it on the trusted application pool you created in step 1. Verify that SEFAUtil is running correctly by running it to display the call forwarding settings of a user in the deployment.	RTCUniversalServerAdmins	<a href="#">Deploy the SEFAUtil tool in Skype for Business</a> <a href="#">New-CsTrustedApplicationPool</a> <a href="#">New-CsTrustedApplication</a> <a href="#">Enable-CsTopology</a> <a href="#">Skype for Business Server 2015 Resource Kit Tools Documentation</a> . (For Skype for Business Server you must use the current version of the tool, but this documentation from Lync Server 2013 still applies.)
Configure call pickup number ranges in the call park orbit table	Use the <b>New-CSCallParkOrbit</b> cmdlet to create call pickup number ranges in the call park orbit table and assign the call pickup ranges the type <b>GroupPickup</b> . For seamless integration with existing dial plans, number ranges are typically configured as a block of virtual extensions. Assigning Direct Inward Dialing (DID) numbers as range numbers in the call park orbit table is not supported.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	<a href="#">Create or modify a Group Call Pickup number range in Skype for Business</a>

PHASE	STEPS	REQUIRED GROUPS AND ROLES	DEPLOYMENT DOCUMENTATION
Assign a call pickup number to users, and enable Group Call Pickup for the users	Use the /enablegrouppickup parameter in the SEFAUtil resource kit tool to enable Group Call Pickup and assign a call pickup number for users.	-	<a href="#">Enable Group Call Pickup for users and assign a group number in Skype for Business</a>
Notify users of their assigned call pickup number and any other number of interest	After you enable Group Call Pickup for users, use email or some other mechanism to notify users of their call pickup group number. Notify users of the call pickup group number for any group that they might want to monitor. Because users can retrieve calls for other users even if they are not in the same group, users might need the call pickup group number for multiple groups.	-	
Verify your Group Call Pickup deployment	Test placing and retrieving calls to make sure that your configuration works as expected. At a minimum, verify the following: Call a user who is enabled for Group Call Pickup and have another user retrieve the call. The other user can be in the same group, in a different group, or not have Group Call Pickup enabled. Call a user who is enabled for Group Call Pickup and do not answer the call.	-	

# Deploy the SEFAUtil tool in Skype for Business

8/7/2019 • 2 minutes to read

Deploying the SEFAUtil tool in Skype for Business Server.

To deploy and manage Group Call Pickup, you need to use the Skype for Business Server version of the SEFAUtil tool.

## IMPORTANT

Microsoft Unified Communications Managed API (UCMA) 5 Runtime must be installed on any computer where you plan to run the SEFAUtil tool. Download it here: [Unified Communications Managed API 5.0 Runtime](#). You can also download the UCMA 5 SDK, which includes the runtime, here: [UCMA 5.0 SDK](#).

You can run the SEFAUtil tool in any Front End pool in your deployment. To run the SEFAUtil tool you must run Steps 1, 2, and 3 from the Skype for Business Deployment Wizard on the Trusted Application Computer. SEFAUtil requires the local configuration store to be present, as well as a certificate.

## NOTE

For more details about running SEFAUtil, see the blog article, "[How to get SEFAUtil running?](#)".

## To deploy SEFAUtil

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. The SEFAUtil tool can be run only on a computer that is part of a trusted application pool. If needed, define a trusted application pool for the Front End pool where you plan to run SEFAUtil. At the command line, run:

```
New-CsTrustedApplicationPool -id <Pool FQDN> -Registrar <Pool Registrar FQDN> -site Site:<Pool Site>
```

## NOTE

Pool FQDN: The FQDN of the server or pool that will host the SEFAUtil application (usually a Skype for Business Front End server or pool). Pool Registrar FQDN: The FQDN of the Skype for Business Front End server or pool associated with this application pool. Pool Site: The Site ID of the site on which this pool is homed.

4. Define the SEFAUtil tool as a trusted application. At the command line, run:

```
New-CsTrustedApplication -ApplicationId sefautil -TrustedApplicationPoolFqdn <Pool FQDN> -Port 7489
```

**NOTE**

You can use a different port if needed.

5. Enable the topology with your changes. At the command line, run:

```
Enable-CsTopology
```

6. If you haven't already, download the Skype for Business Server version of the SEFAUtil tool from [this location](#), and install it on the trusted application pool you created in step 3.
7. Verify that the SEFAUtil tool is running correctly, as follows:
  - a. Run the tool from the Windows command prompt with administrator privileges to display the call forwarding settings of a user in your deployment.
  - b. Display the call forwarding settings of a user. At the command line, run:

```
SEFAUtil.exe <user SIP address> /server:<Lync Server/Pool FQDN>
```

The call forwarding settings for the user will be displayed.

# Create or modify a Group Call Pickup number range in Skype for Business

8/7/2019 • 3 minutes to read

Create or modify a Group Call Pickup number range in Skype for Business Server Enterprise Voice.

Group Call Pickup is based on the Call Park application. When you deploy Group Call Pickup, you must configure the call park orbit table with ranges of phone numbers that are designated as call pickup group numbers. These group numbers are the numbers that users dial to pick up calls that are ringing for another user.

Like call park orbit numbers, call pickup group numbers need to be virtual extensions that have no user or phone assigned to them. Each Front End pool where you deploy Group Call Pickup can have one or more ranges of call pickup group numbers. The group number ranges must be globally unique in your deployment, and must be assigned as the **GroupPickup** type.

Use the following procedure to create or modify a call pickup group number range in the call park orbit table.

## NOTE

You must use Skype for Business Server Management Shell to create, modify, remove, and view Group Call Pickup number ranges in the call park orbit table. Group Call Pickup number ranges are not available in Skype for Business Server Control Panel.

The call pickup group number ranges must comply with the following rules:

- The beginning number of the range must be less than or equal to the ending number of the range.
- The value of the beginning number of the range must be the same length as the ending number of the range.
- The number range must be unique. This range cannot overlap with any other range.
- If the number range begins with the character \* or #, the range must be greater than 100.
- Valid values: Must match the regular expression string  $([\*|\#]?[1-9]\d{0,7})|([1-9]\d{0,8})$ . This means the value must be a string beginning with either the character \* or # or a number 1 through 9 (the first character cannot be a zero). If the first character is \* or #, the following character must be a number 1 through 9 (it cannot be a zero). Subsequent characters can be any number 0 through 9 up to seven additional characters (for example, "#6000", "\*92000", "\*95551212", and "915551212"). If the first character is not \* or #, the first character must be a number 1 through 9 (it cannot be zero), followed by up to eight characters, each a number 0 through 9 (for example, "915551212", "41212", "300").

## To create or modify a call pickup group range

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Use **New-CsCallParkOrbit** to create a new range of call pickup group numbers. Use **Set-CsCallParkOrbit** to modify an existing range of call pickup numbers.

At the command line, run:

```
New-CsCallParkOrbit -Identity <name of call pickup group range> -NumberRangeStart <first number in range> -NumberRangeEnd <last number in range> -CallParkService <FQDN or service ID of the Application service that hosts the Call Park application> -Type GroupPickup
```

For example:

```
New-CsCallParkOrbit -Identity "Redmond call pickup" -NumberRangeStart 100 -NumberRangeEnd 199 -CallParkService redmond-applicationserver-1 -Type GroupPickup
```

The following example shows how to change a range of numbers from call park orbits to call pickup groups.

```
Set-CsCallParkOrbit -Identity "Redmond call pickup" -Type GroupPickup
```

#### **IMPORTANT**

Use this cmdlet to change the type assigned to number ranges only if you initially specified the incorrect type and the group range is not yet in use. If you change the number range from CallPark to GroupPickup or vice versa and the number range is already in use, either Call Park or Group Call Pickup will stop working for that number range. For example, if you change a number range from CallPark to GroupPick, the Call Park application can no longer use that range of orbits to park calls.

## See also

[New-CsCallParkOrbit](#)

[Set-CsCallParkOrbit](#)

[Delete a Call Park Orbit Range](#)

# Enable Group Call Pickup for users and assign a group number in Skype for Business

8/7/2019 • 2 minutes to read

Enable users for Group Call Pickup in Skype for Business Server Enterprise Voice, and assign a group number.

After you add call pickup group numbers to the call park orbit table, you use the SEFAUtil tool to assign the group numbers to users and enable Group Call Pickup for them.

## NOTE

In a hybrid deployment, do not assign a Group Call Pickup group to users who are homed online. Users who are homed online cannot participate in Group Call Pickup. That is, their calls cannot be answered by other users, and they cannot answer calls to other users.

## To assign a group number and enable Group Call Pickup for a user

1. Log on to the computer where you installed the SEFAUtil tool with administrator rights.
2. At the command line, run:

```
SEFAUtil.exe sip:<sip address of user> /server:<pool FQDN> /enablegrouppickup:<group number>
```

For example, to assign group number 199 to a user:

```
SEFAUtil.exe katarina@contoso.com /server:pool01.contoso.com /enablegrouppickup:199
```

## See also

[Disable Group Pickup for Users](#)



# Deployment process for Response Group in Skype for Business

8/7/2019 • 7 minutes to read

Deployment process and steps for Response Group in Skype for Business Server Enterprise Voice.

Response Group is an Enterprise Voice feature that routes and queues incoming calls to groups of people, called agents, such as a help desk or a customer service desk.

The components that Response Group requires are installed and enabled automatically on the Front End Server or Standard Edition server when you deploy Enterprise Voice. To make Response Group available to users, you must configure agent groups, then queues, and then workflows. Additionally, a Response Group Administrator can delegate configuration of an existing workflow to a Response Group Manager, who can then modify and reconfigure the workflow and its associated agent groups and queues.

To configure response groups, you must be a member of at least one of the following administrative roles:

ACTIVE DIRECTORY SECURITY GROUP (1)	CREATE WORKFLOW	ASSIGN MANAGER	CREATE /ASSIGN AGENTS, QUEUES	CREATE / MANAGE HOLIDAY AND BUSINESS HOURS	ACTIVATE / DEACTIVATE WORKFLOW	CONFIGURE WORKFLOW (IVR OR HUNT GROUP)
<b>CsResponseGroupAdministrator</b>	√	√	√	√	√	√
<b>CsResponseGroupManager</b>		√(2)	√(3)	√(3)	√(3)	√(3)
<b>CsVoiceAdministrator</b>	√	√	√	√	√	√
<b>CsServerAdministrator</b>	√	√	√	√	√	√
<b>CsAdministrator</b>	√	√	√	√	√	√
<b>CsViewOnlyAdministrator</b>	√(4)	√(4)	√(4)	√(4)	√(4)	√(4)

## NOTE

**(1)** An Active Directory Domain Services user object must be a member of the specified Active Directory security group listed. An administrator or other delegated Active Directory group member with appropriate permissions to add users to a security group (For example, Administrator, Account Operators) must add a user object to the listed security group or group for the user to be able to perform the functions listed. **(2)** Only for workflows that the CsResponseGroupAdministrator has assigned to the CsResponseGroupManager. **(3)** A Response Group Manager can assign another member of CsResponseGroupManager to a workflow that the current manager already manages. **(4)** CsViewOnlyAdministrator can only run verb "Get" cmdlets.

# Response Group Configuration Prerequisites

Response Group requires the following components:

- Application service
- Response Group application
- Language packs
- File store (to hold audio files)
- Web Services (includes the Response Group Configuration Tool and the agents' sign-in and sign-out console)

All of these components are installed by default when you deploy Enterprise Voice.

You might need to perform the following tasks before configuring Response Group:

- Enable users for Lync Server 2013 and Enterprise Voice.
- Modify a configuration file to be compliant with Federal Information Processing Standards (FIPS).
- Modify the database collation to support Yi, Meng, and Zang characters for queue names and agent group names.

## Enabling Users

The first step in configuring Response Group is to create agent groups. Before you can create an agent group, you must enable the users who will be agents for Response Group for Skype for Business and Enterprise Voice. Enabling users for Skype for Business is typically a step in the Enterprise Edition server or Standard Edition server deployment. For details about enabling users for Skype for Business, see [Enable or Disable Users for Lync Server 2013 Preview](#). Enabling users for Enterprise Voice is typically a step in the Enterprise Voice deployment. For details, see [Enable users for Enterprise Voice in Skype for Business Server](#).

## Complying with FIPS requirements

This section applies to you only if your organization needs to comply with Federal Information Processing Standards (FIPS).

To be compliant with FIPS, you need to modify the application-level Web.config file to use a different cryptography algorithm after you install Web Services. You need to specify that ASP.NET use the Triple Data Encryption Standard (3DES) algorithm to process view state data. For the Response Group application, this requirement applies to the Response Group Configuration Tool and the agent sign-in and sign-out console. For details about this requirement, see Microsoft Knowledge Base article 911722, "You may receive an error message when you access ASP.NET webpages that have ViewState enabled after you upgrade from ASP.NET 1.1 to ASP.NET 2.0," at <https://go.microsoft.com/fwlink/p/?linkId=196183>.

To modify the Web.config file, do the following:

1. In a text editor such as Notepad, open the application-level Web.config file.
2. In the Web.config file, locate the `<system.web>` section.
3. Add the following `<machineKey>` section to in the `<system.web>` section:

```
<machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="AutoGenerate,IsolateApps"
validation="3DES" decryption="3DES"/>
```

4. Save the Web.config file.

5. Restart the Internet Information Services (IIS) service by running the following command at a command prompt:

```
iisreset
```

### Supporting Yi, Meng, and Zang Characters

This section applies to you only if your organization needs to support Yi, Meng, or Zang characters.

#### NOTE

For information on what the Yi, Meng, and Zang characters are and why they may be important to your deployment, see the information on the GB18030 character sets <https://go.microsoft.com/fwlink/p/?linkId=240223>.

To support Yi, Meng, or Zang characters, you need to modify the collation for the Rgsconfig database. Change the collation of the **Name** column in the following tables in each Rgsconfig database:

- dbo.AgentGroups
- dbo.BusinessHours
- dbo.HolidaySets
- dbo.Queues
- dbo.Workflows

For SQL Server 2008 R2 and SQL Server 2012, use the Latin\_General\_100 (Accent Sensitive) collation. If you use this collation, all object names are not case-sensitive.

You can change the collation by using Microsoft SQL Server Management Studio. For details about using this tool, see "[Using SQL Server Management Studio](#)". Follow these steps to change the collation:

1. Be sure that SQL Server Management Studio is configured to allow changes that require tables to be recreated. For details, see "[Save \(Not Permitted\) Dialog Box](#)". For details about setting a column collation, see at "[How to: Set Column Collation \(Visual Database Tools\)](#)".
2. Using Microsoft SQL Server Management Studio, connect to the Rgsconfig database.
3. Find the table you want to change in the Rgsconfig database, right-click the table, and click **Design**.
4. Change the collation of the **Name** column and save the table.

## Response Group deployment steps

### Response Group Deployment Process

PHASE	STEPS	PERMISSIONS	DEPLOYMENT DOCUMENTATION
-------	-------	-------------	--------------------------

PHASE	STEPS	PERMISSIONS	DEPLOYMENT DOCUMENTATION
<p>Enable users for Skype for Business and for Enterprise Voice</p>	<p>Enable users who will be agents for Skype for Business and Enterprise Voice. Users must be enabled before you can add them to agent groups. Typically, users are enabled for Skype for Business during the Enterprise Edition or Standard Edition server deployment. Users are enabled for Enterprise Voice during the Enterprise Voice deployment.</p>	<p>RTCUniversalUserAdmins CsUserAdministrator CsAdministrator</p>	<p><a href="#">Enable or Disable Users for Lync Server 2013 Preview</a> <a href="#">Enable users for Enterprise Voice in Skype for Business Server</a></p>
<p>Create and configure response groups, which consist of agent groups, queues, and workflows</p>	<ol style="list-style-type: none"> <li>1. Use the Skype for Business Server Control Panel or Skype for Business Server Management Shell to do the following: <ol style="list-style-type: none"> <li>a. Create and configure agent groups.</li> <li>b. Create and configure queues.</li> </ol> </li> <li>2. Optionally, use Skype for Business Server Management Shell to create predefined response group business hours and holidays.</li> <li>3. Use the Response Group Configuration Tool or Skype for Business Server Management Shell to create workflows (hunt groups or interactive voice response (IVR) call flows), including custom response group business hours and holidays. You can access the Response Group Configuration Tool through Skype for Business Server Control Panel.</li> </ol>	<p>RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator CsResponseGroupManager</p>	<p><a href="#">Create Response Group Agent Groups</a> <a href="#">Create Response Group Queues</a> <a href="#">(Optional) Define Response Group business hours in Skype for Business</a> <a href="#">(Optional) Define Response Group holiday sets in Skype for Business</a> <a href="#">Designing and creating response group workflows in Skype for Business</a></p>
<p>(Optional) Customize application-level settings</p>	<p>Use Skype for Business Server Management Shell to customize the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration.</p>	<p>RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator</p>	<p><a href="#">Managing application-level Response Group settings in Skype for Business</a></p>

PHASE	STEPS	PERMISSIONS	DEPLOYMENT DOCUMENTATION
(Optional) Delegate management of response groups	Assign users the CsResponseGroupManager role to delegate configuration of response groups. Response Group Managers can then configure the response groups assigned to them.	RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator	<a href="#">Planning for Role-Based Access Control</a>
Verify your Response Group deployment	Test answering calls to your hunt group and interactive voice response workflows to ensure that your configuration works as expected.	-	-

## Overview of workflow creation scenarios

When you create workflows, there are two possible scenarios:

- **The Administrator creates and configures the workflow** — The CsResponseGroupAdministrator role member (or equivalent) creates and activates the workflow and all elements in the workflow, such as the agent groups, queues, holiday and business hours, music on hold, and so on.
- **The Administrator creates the workflow and the Manager configures options** — The CsResponseGroupAdministrator role member (or equivalent) defines the primary SIP URI, Display Name, assigns a member or members of the CsResponseGroupManager role, and selects a queue and activates the workflow. The CsResponseGroupManager can then log on and edit the configuration of the workflow by creating agent groups and also assigns the group to the queue, configuring the telephone number, holiday and business hours, music on hold, and so on.

### NOTE

When you want to create a managed workflow, you need to create the workflow as active. After you save an active, managed workflow, you can then modify and deactivate the workflow.

# Create or modify an agent group in Skype for Business

8/7/2019 • 7 minutes to read

Create or modify an agent group in Response Group, in Skype for Business Server Enterprise Voice.

When you create an agent group, you select the agents that are assigned to the group and specify additional group settings, such as the routing method and whether an agent can sign in to and out of the group.

An agent who must sign in and out of the group, which is different from signing in or out of Skype for Business, is called a formal agent. Formal agents must be signed in to the group before they can receive calls routed to the group. This can be useful for agents who answer calls from the group on a part-time basis. Formal agents sign in and out of their groups by clicking a menu item in Skype for Business to open the Windows Internet Explorer Internet browser and display a webpage console.

An agent who does not sign in or out of the group is called an informal agent. Informal agents are automatically signed in to the group when they sign in to Skype for Business, and they cannot sign out of the group.

Only on-premises users can be agents. If an agent is moved from on-premises to online, Response Group calls will not be routed to that agent.

Use one of the following procedures to create or modify an agent group.

## IMPORTANT

When you assign users as response group agents, inform them that, if they have Privacy mode enabled, they need to search for "RGS Presence Watcher" contacts and add them to their Contacts list. Agents who have Privacy mode enabled, but who do not have "RGS Presence Watcher" in their Contacts list, cannot receive calls to the response group. Agents who do not have Privacy mode enabled are not affected.

## To use Skype for Business Server Control Panel to create or modify an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

## NOTE

If you are one of the delegated Response Group Managers for a managed workflow, you can create groups and use them in the workflows that you manage.

2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Response Groups**, and then click **Group**.
4. On the **Group** page, do one of the following:
  - To create a new agent group, click **New**. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service where you want to add the group. In the resulting list of services, click the service that you want, and then click **OK**.
  - To modify an existing agent group, type all or part of the name of the agent group in the search field.

In the resulting list, click the group that you want, click **Edit**, and then click **Show details**.

5. In **Name**, type an identifying name for the agent group.
6. In **Description**, type a description for the group.
7. In the **Participation policy**, select one of the following to set up the sign-in behavior for the group:
  - Select **Informal** to specify that agents in the group do not need to sign in and out of the group. Agents are automatically signed in to the group when they sign in to Skype for Business.
  - Select **Formal** to specify that agents in the group must sign in and out of the group. When you select this option, agents click a menu item in Skype for Business to open Internet Explorer and display a webpage console for signing in and out of the group.
8. In **Alert time (seconds)**, specify the number of seconds to ring an agent before offering the call to the next available agent (the default is 20 seconds).

#### **IMPORTANT**

The agent alert time setting cannot exceed 180 seconds. If the agent alert time exceeds 180 seconds, the client application rejects the call because the SIP transaction timer reaches its maximum wait time.

9. In **Routing method**, select the method for routing calls to agents in the group as follows:
  - To offer a new call first to the agent who has been idle the longest (has had a presence of **Available** or **Inactive** in Skype for Business the longest), click **Longest idle**.
  - To offer a new call to all available agents at the same time, click **Parallel**. The call is sent to the first agent who accepts it.
  - To offer a new call to each agent in turn, click **Round robin**.
  - To always offer a new call to the agents in the order in which they are listed in the **Agent** list, click **Serial**.
  - To offer a new call to all agents who are signed into Skype for Business and the Response Group application at the same time, regardless of their current presence, click **Attendant**. Users who are configured as agents can see all the calls that are waiting and answer waiting calls in any order. The call is sent to the first agent who accepts it, after which the other agents no longer see the call.
10. In **Agents**, specify how you want to create your agents list:
  - To use a custom list of agents, click **Define a custom group of agents**, and do one of the following:
    - To add a user to the agent group, click **Select**, and then in the **Select Agents** search field, type all or part of the name of the user that you want to add to this group, and then click **Find**. In the resulting list of agents, click the user, and then click **OK**.
    - To remove a user from the agent group, in the list of agents, click the user you want to remove, and then click **Remove**.
    - To change the order in which agents are offered calls in groups that use either round robin routing or serial routing, in the list of agents, click a user, and then click the up arrow or down arrow.
    - To use a Microsoft Exchange Server distribution list as your agent group, click **Use an existing email distribution list**, and then in **Distribution list address**, type the email address of the distribution list (for example, NetworkSupport@contoso.com).

If you use an email distribution list, you are subject to the following constraints:

- You cannot select multiple distribution lists for the agent group. Each group supports only a single distribution list.
- If the distribution list contains one or more distribution lists, members of the nested distribution lists are not added to the agent list.
- If serial or round robin routing is selected, the server offers an incoming call to the appropriate agent according to the routing method and according to the order in which agents are listed in the distribution list.
- If the distribution list contains users for which Lync Server 2010 is enabled but Enterprise Voice is not enabled, they will be added to the agent group as dysfunctional agents. Make sure that all members of the distribution list have Enterprise Voice enabled for their user accounts.

#### IMPORTANT

If you use an email distribution list, hidden memberships or hidden lists might become visible to the Response Group administrator or users.

Hidden memberships or hidden lists can become visible as follows:

- If a distribution list was configured so that the membership is hidden and the Response Group administrator assigns the distribution list to the agent list, users can call the group to find out who the members are.
- If a distribution list was configured so that it is hidden in the Exchange Global Address List, the Response Group administrator might be able to see the distribution list and assign it to the agent list if the Response Group process has the appropriate user rights and permissions, even if the administrator does not have the appropriate user rights and permissions.

#### 11. Click **Commit**.

#### To use Skype for Business Server Management Shell to create or modify an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Use **New-CsRgsAgentGroup** to create a new agent group. Use **Set-CsRgsAgentGroup** to modify an existing agent group. At the command line, run:

```
New-CsRgsAgentGroup -Name "<agent group name>" -Parent $serviceId [-Description "<agent group description>"] [-AgentAlertTime <# seconds until call is routed to next agent>] [-ParticipationPolicy <Formal | Informal>] [-RoutingMethod <method for routing calls>] [-AgentsByUri("<first agent's SIP address>","<second agent's SIP address>")];
```

For example:

```
New-CsRgsAgentGroup -Name "Help Desk" -Parent "service:ApplicationServer:atl-cs-001.contoso.com" -Description "Contoso Help Desk" -AgentAlertTime 20 -ParticipationPolicy Formal -RoutingMethod RoundRobin -AgentsByUri("sip:mindy@contoso.com","sip:bob@contoso.com")
```



**IMPORTANT**

The agent alert time setting cannot exceed 180 seconds. If the agent alert time is greater than 180 seconds, the client application rejects the call because the SIP transaction timer reaches its maximum wait time.

4. Confirm that the agent group is created. Run:

```
Get-CsRgsAgentGroup -Name "Help Desk"
```

## See also

[Get-CsService](#)

[New-CsRgsAgentGroup](#)

[Set-CsRgsAgentGroup](#)

[Get-CsRgsAgentGroup](#)

# Create or modify a queue in Skype for Business

8/7/2019 • 6 minutes to read

Create or modify a Response Group queue, in Skype for Business Server Enterprise Voice.

Queues hold callers until an agent answers the call. When the Response Group application searches for an available agent, it searches agent groups in the order that you list them. You can select the agent groups that are assigned to the queue and specify queue behavior, such as limiting the number of calls that the queue can hold and the period of time that a call waits until an agent answers the call.

Use one of the following procedures to create or modify a queue.

## To use Skype for Business Server Control Panel to create or modify a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

### NOTE

If you are one of the delegated Response Group Managers for a managed workflow, you can create or modify response group queues and assign them to the workflows that you manage.

2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Response Groups**, and then click **Queue**.
4. On the **Queue** page, do one of the following:
  - To create a new queue, click **New**. In **Select a Service**, type part or all of the name of the **ApplicationServer** service where you want to add the queue in the search field. In the resulting list of services, click the service that you want, and then click **OK**.
  - To modify an existing queue, type all or part of the queue name in the search field. In the resulting list of queues, click the queue that you want, click **Edit**, and then click **Show details**.
5. In **Name**, type an identifying name for the queue.
6. In **Description**, type a description for the queue.
7. In **Groups**, specify the groups you want to assign to the queue. Do one of the following:
  - To add a group to the queue, click **Select**. In the **Select Groups** search field, type all or part of the name of the agent group that you want to assign to the queue, click the agent group that you want, and then click **OK**.
  - To remove a group from the queue, in the list of agent groups, click the group that you want to remove, and then click **Remove**.
  - To change the order in which agents are searched, in the list of agent groups, click a group, and then click the up arrow or down arrow.

#### NOTE

When the server searches for an available agent for the queue, it uses group order. That is, the first group in the list is searched first, followed by the second group in the list, and so on.

8. To specify a maximum period of time for a caller to wait on hold before an agent answers the call, select the **Enable queue time-out** check box, and then do the following:
  - a. In **Time-out period (seconds)**, specify the maximum number of seconds a caller waits for an agent to answer the call.
  - b. In **Call Action**, select the action that occurs when a call times out as follows:
    - To disconnect the call after the timeout, click **Disconnect**.
    - To forward the call to voice mail, click **Forward to voice mail**, and then in the **SIP address** field, type a voice mail address in the format sip: <username>@ <domainname> (for example, sip:bob@contoso.com).
    - To forward the call to another telephone number, click **Forward to telephone number**, and then in the **SIP address** field, type the telephone number in the format sip: <number>@ <domainname> (for example, sip:+14255550121@contoso.com).
    - To forward the call to another user, click **Forward to SIP address**, and then in the **SIP address** field, type the URI for the user in the format sip: <username>@ <domainname>.
    - To forward the call to another queue, click **Forward to another queue**, and then browse to the queue that you want to use.
9. To specify a maximum number of calls that the queue can hold, select the **Enable queue overflow** check box, and then do the following:
  - a. In **Maximum number of calls**, select the maximum number of calls that you want the queue to hold.
  - b. In **Forward the call**, select which call is to be forwarded when the queue is full: **Newest Call** or **Oldest Call**.
  - c. In **Call action**, select the action that occurs when the overflow threshold is met as follows:
    - To disconnect the call after the timeout, click **Disconnect**.
    - To forward the call to voice mail, click **Forward to voice mail**, and then in the **SIP address** field, type a voice mail address in the format sip: <username>@ <domainname> (for example, sip:bob@contoso.com).
    - To forward the call to another telephone number, click **Forward to telephone number**, and then in the **SIP address** field, type the telephone number in the format sip: <number>@ <domainname> (for example, sip:+14255550121@contoso.com).
    - To forward the call to another user, click **Forward to SIP address**, and then in the **SIP address** field, type the URI for the user in the format sip: <username>@ <domainname>.
    - To forward the call to another queue, click **Forward to another queue**, and then browse to the queue that you want to use.
10. Click **Commit**.

#### To use Skype for Business Server Management Shell to create or modify a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined

administrative roles that support Response Group.

#### NOTE

If you are one of the delegated Response Group Managers for a managed workflow, you will be able to create agent groups and queues, and assign agent groups to queues.

2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Create the prompt to be played when the queue timeout threshold is met, and save it in a variable. At the command line, run:

```
$promptTO = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>"
```

For example:

```
"All agents are currently busy. Please call back later."
```

#### NOTE

To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see [Import-CsRgsAudioFile](#).

4. Define the action to be taken when the queue timeout threshold is met, and save it in a variable. At the command line, run:

```
$actionTO = New-CsRgsCallAction -Prompt <saved prompt from previous step> -Action <action to be taken>
```

#### NOTE

For details about possible actions and their syntax, see [New-CsRgsCallAction](#).

For example:

```
$action = New-CsRgsCallAction -Prompt $promptTO -Action Terminate
```

5. Create the prompt to be played when the queue overflow threshold is met, and save it in a variable. At the command line, run:

```
$promptOV = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>"
```

For example:

```
$promptOV = New-CsRgsPrompt -TextToSpeechPrompt "Too many calls are waiting. Please call back later."
```

#### NOTE

To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see [Import-CsRgsAudioFile](#).

- Define the action to be taken when the queue overflow threshold is met, and save it in a variable. At the command line, run:

```
$actionOV = New-CsRgsCallAction -Prompt <saved prompt from previous step> -Action <action to be taken>
```

#### NOTE

For details about possible actions and their syntax, see [New-CsRgsCallAction](#).

For example:

```
$action = New-CsRgsCallAction -Prompt $promptOV -Action Terminate
```

- Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId="service:"+(Get-CSService | ?{$_ .Applications -Like "*RGS*"}).ServiceId;
```

- Get the identity of the agent group to be assigned to the queue. At the command line, run:

```
$agid = (Get-CsRgsAgentGroup -Name "Help Desk").Identity;
```

#### NOTE

For details about creating the agent group, see [New-CsRgsAgentGroup](#)

- Create the queue. At the command line, run:

```
$q = New-CsRgsQueue -Parent <saved service ID from previous step> -Name "<name of queue>" [-Description "<description for queue>"] [-TimeoutThreshold <# seconds before call times out>] [-TimeoutAction <saved timeout action>] [-OverflowThreshold <# calls queue can hold>] [-OverflowCandidate <call to be acted on when overflow threshold met>] [-OverflowAction <saved overflow action>] [-AgentGroupIDList(<agent group identity>)];
```

For example:

```
$q = New-CsRgsQueue -Parent $serviceId -Name "Help Desk" -Description "Contoso Help Desk" -TimeoutThreshold 300 -TimeoutAction $actionTO -OverflowThreshold 10 -OverflowCandidate NewestCall -OverflowAction $actionOV -AgentGroupIDList($agid.Identity);
```

- Confirm that the queue is created. Run:

```
Get-CsRgsQueue -Name "Help Desk"
```

## See also

[New-CsRgsQueue](#)

[Set-CsRgsQueue](#)

New-CsRgsPrompt

New-CsRgsCallAction

Get-CsRgsQueue

Import-CsRgsAudioFile

Remove-CsRgsQueue

# (Optional) Define Response Group business hours in Skype for Business

8/7/2019 • 2 minutes to read

Create or modify Response Group business hours, in Skype for Business Server Enterprise Voice.

## Defining Business Hours

Business hour settings define when the workflow is available to answer calls and specify the actions to take for calls outside of business hours. Response Group administrators can use the **New-CsRgsHoursOfBusiness** cmdlet to create predefined schedules that you can use for any number of response groups.

### TIP

When you create or modify a workflow, you can specify a custom schedule that applies only to that workflow. For details, see [Designing and creating response group workflows in Skype for Business](#).

### NOTE

If a workflow is defined as a Managed workflow, then any user who is assigned the CsResponseGroupManager role can set and modify custom business hours for workflows that they manage.

### IMPORTANT

Use 24-hour notation for the parameters in the following cmdlets (for example, 20:00=8:00 P.M.).

### To create a predefined business hours collection

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. For each unique range of hours you want to define, run:

```
$x = New-CsRgsTimeRange [-Name <name of time range>] -OpenTime <time when business hours begin> -  
CloseTime <time when business hours end>
```

To create the business hours collection that uses the ranges you defined, run:

```
New-CsRgsHoursOfBusiness -Parent <service where the workflow is hosted> -Name <unique name for collection> [-MondayHours1 <first set of opening and closing times for Monday>] [-MondayHours2 <second set of opening and closing times for Monday>] [-TuesdayHours1 <first set of opening and closing times for Tuesday>] [-TuesdayHours2 <second set of opening and closing times for Tuesday>] [-WednesdayHours1 <first set of opening and closing times for Wednesday>] [-WednesdayHours2 <second set of opening and closing times for Wednesday>] [-ThursdayHours1 <first set of opening and closing times for Thursday>] [-ThursdayHours2 <second set of opening and closing times for Thursday>] [-FridayHours1 <first set of opening and closing times for Friday>] [-FridayHours2 <second set of opening and closing times for Friday>] [-SaturdayHours1 <first set of opening and closing times for Saturday>] [-SaturdayHours2 <second set of opening and closing times for Saturday>] [-SundayHours1 <first set of opening and closing times for Sunday>] [-SundayHours2 <second set of opening and closing times for Sunday>]
```

The following example specifies business hours of 9:00 A.M. to 5:00 P.M. for weekdays, 8:00 A.M. to 10:00 A.M. and again from 2:00 P.M. to 6:00 P.M. for Saturdays, and no business hours for Sundays:

```
$a = New-CsRgsTimeRange -Name "Weekday Hours" -OpenTime "9:00" -CloseTime "17:00"  
$b = New-CsRgsTimeRange -Name "Saturday Morning Hours" -OpenTime "8:00" -CloseTime "10:00"  
$c = New-CsRgsTimeRange -Name "Saturday Afternoon Hours" -OpenTime "14:00" -CloseTime "18:00"  
New-CsRgsHoursOfBusiness -Parent "ApplicationServer:Redmond.contoso.com" -Name "Help Desk Business Hours" -MondayHours1 $a -TuesdayHours1 $a -WednesdayHours1 $a -ThursdayHours1 $a -FridayHours1 $a -SaturdayHours1 $b -SaturdayHours2 $c
```

## See also

[New-CsRgsTimeRange](#)

[New-CsRgsHoursOfBusiness](#)



# (Optional) Define Response Group holiday sets in Skype for Business

8/7/2019 • 2 minutes to read

Create or modify Response Group holiday sets, in Skype for Business Server Enterprise Voice.

Holiday settings define the days that a response group is closed for business and specify the action to take on those days. A holiday set is the collection of holidays that apply to a response group.

## NOTE

If a workflow is defined as a Managed workflow, then any user is assigned the CsResponseGroupManager role can set and modify holidays for workflows that they manage.

## To create a holiday set

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. For each holiday you want to define, run:

```
$x = New-CsRgsHoliday [-Name <holiday name>] -StartDate <starting date of holiday> -EndDate <ending date of holiday>
```

To create the holiday set that contains the holidays you defined, run:

```
New-CsRgsHolidaySet -Parent <service where the workflow is hosted> -Name <unique name for holiday set> -HolidayList <one or more holidays to be included in the holiday set>
```

The following example shows a holiday set that includes two holidays:

```
$a = New-CsRgsHoliday -Name "New Year's Day" -StartDate "1/1/2018 12:00 AM" -EndDate "1/2/2018 12:00 AM"  
$b = New-CsRgsHoliday -Name "Independence Day" -StartDate "7/4/2018 12:00 AM" -EndDate "7/5/2018 12:00 AM"  
New-CsRgsHolidaySet -Parent "ApplicationServer:Redmond.contoso.com" -Name "2018 Holidays" -HolidayList ($a, $b)
```

## See also

[Designing and creating response group workflows in Skype for Business](#)

[New-CsRgsHoliday](#)

[New-CsRgsHolidaySet](#)

# Designing and creating response group workflows in Skype for Business

8/7/2019 • 33 minutes to read

Design and create Response Group workflows, in Skype for Business Server Enterprise Voice. Both hunt group workflows and interactive workflows are covered.

A workflow defines the behavior of a call from the time that the phone rings to the time that someone answers the call. The workflow specifies the queue to use for holding the call, and specifies the routing method to use for hunt group workflows or the questions and answers to use for interactive response group workflows.

A workflow also defines settings such as a welcome message, music on hold, business hours, and holidays.

## NOTE

You must create agent groups and queues before you create a workflow that uses them.

## Creating or modifying a hunt group workflow

### To use Response Group Configuration Tool to create or modify a hunt group workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service that hosts the workflow that you want to create or change. In the resulting list of services, click the service that you want, and then click **OK**.

## NOTE

The Response Group Configuration Tool opens. You can also open the Response Group Configuration Tool directly from a web browser by typing the following URL: `https://<webPoolFqdn>/RgsConfig`.

6. Do one of the following:
  - Under **Create a New Workflow**, next to **Hunt Group**, click **Create**.
  - Under **Manage an Existing Workflow**, locate the workflow you want to change, and then under **Action**, click **Edit**.
7. If you are ready for users to start calling the workflow, select **Activate the workflow**.

**NOTE**

If you are creating a managed workflow, you need to select **Activate the workflow**. After you save the active, managed workflow, you can then modify and deactivate it.

- To allow federated users to call the group, select the **Enable for federation** check box. You must also have an external access policy that applies to the Response Group application configured for federation.

**NOTE**

The global external access policy applies to the Response Group application. You can configure the global policy for response group federation by using Skype for Business Server Control Panel or by using the **Set-CsExternalAccessPolicy** cmdlet to set the EnableOutsideAccess parameter to True. Keep in mind that global policy settings apply to all users unless they are assigned a site or user policy. Therefore, before changing this setting for response groups, make sure that the federation setting meets the requirements of your organization. For details about how policies apply to users, see [Manage External Access Policy for Your Organization](#). For details about the federation setting, see [Set-CsExternalAccessPolicy](#).

**NOTE**

Users who are hosted in Skype for Business Online can't place calls to response groups that are hosted in an on-premises deployment. This is true in both hybrid deployments and in cases where an on-premises deployment is federated with a Skype for Business Online deployment.

- To hide the identity of agents during calls, select the **Enable agent anonymity** check box.

**NOTE**

Anonymous calls cannot start with instant messaging (IM) or video, although the agent or the caller can add IM and video after the call is established. An anonymous agent can also put calls on hold, transfer calls (both blind and consultative transfers), and park and retrieve calls. Anonymous calls do not support conferencing, application sharing and desktop sharing, file transfer, whiteboarding and data collaboration, and call recording. Agents using the Lync VDI Plugin can receive incoming calls anonymously, but they cannot make outgoing calls anonymously.

- Under **Enter the address of the group that will receive the calls**, type the primary SIP uniform resource identifier (URI) address of the group that will answer calls to the workflow.

**NOTE**

The primary URI for a workflow is how the workflow is identified and referenced. The SIP URI that you enter is created as a contact object in Active Directory Domain Services. To create the URI, the object must be unique in Active Directory.

- In **Display name**, type the name that you want to display for the workflow (for example, Sales Response Group).

**NOTE**

Do not include the "<" or ">" characters in the display name. Do not use the following display names because they are reserved: **RGS Presence Watcher** or **Announcement Service**.

12. Under **Telephone number**, type the line URI for the response group (for example, +14255550165).
13. In **Display number**, type the number as you want it to appear for the response group (for example, +1 (425) 555-0165).
14. (Optional) In **Description**, type a description for the workflow as you want it to appear on the contact card in Skype for Business.
15. In **Workflow Type**, select **Managed** if this workflow will be managed by a Response Group Manager. Do the following to assign Response Group Managers to the workflow:
  - a. Type the SIP URI of a manager for this workflow, and click **Add**.
  - b. Type the SIP URI of additional managers to add to the workflow, and click **Add**.

#### IMPORTANT

Every user who is designated as a manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

16. Under **Step 2 Select a Language**, click the language that you want to use for speech recognition and text-to-speech.
17. If you want to configure a welcome message, under **Step 3 Configure a Welcome Message**, select the **Play a welcome message** check box, and then do one of the following:
  - To enter the welcome message as text that is converted to speech for callers, click **Use text-to-speech**, and then type the welcome message in the text box.

#### NOTE

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use a wave (.wav) or Windows Media audio (.wma) file recording for the welcome message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the audio file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

#### NOTE

All user-provided audio files must meet certain requirements. For details about supported file formats, see [Technical Requirements for Response Groups](#).

18. Under **Step 4 Specify Your Business Hours**, in **Your time zone**, click the time zone for the workflow.

#### NOTE

The time zone is the time zone where the callers and agents of the workflow reside. It is used to calculate the open and close hours. For example, if the workflow is configured to use the North American Eastern Time zone and the workflow is scheduled to open at 7:00 A.M. and close at 11:00 P.M., the open and close times are assumed to be 7:00 Eastern Time and 23:00 Eastern Time respectively. (You must enter the times in 24-hour time notation.)

19. Select the type of business hours schedule you want to use by doing one of the following:
  - To use a predefined schedule of business hours, click **Use a preset schedule**, and then select the schedule you want to use from the drop-down list.

**NOTE**

You must have defined at least one preset schedule previously to be able to select this option. You define preset schedules by using the **New-CSRgsHoursOfBusiness** cmdlet. For details, see [\(Optional\) Define Response Group business hours in Skype for Business](#).

**NOTE**

When you select a preset schedule, **Day**, **Open**, and **Close** are automatically filled with the days and hours that the response group is available.

- To use a custom schedule that applies only to this workflow, click **Use a custom schedule**.
20. If you are creating a custom schedule for this workflow, click the check boxes for the days of the week that the response group is available.
  21. If you are creating a custom schedule, type the **Open** and **Close** hours for each day of the week that the response group is available.

**NOTE**

The **Open** and **Close** hours must be in 24-hour time notation. For example, if your office works a 9-to-5 work day and closes at noon for lunch, the business hours are specified as **Open** 9:00, **Close** 12:00, **Open** 13:00, and **Close** 17:00.

22. If you want to play a message when the office is not open, select the **Play a message when the response group is outside of business hours** check box, and then specify the message to play by doing one of the following:
  - To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

**NOTE**

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

**NOTE**

All user-provided audio files must meet certain requirements. For details about supported audio file formats, see [Technical Requirements for Response Groups](#).

23. Specify how to handle calls after the message is played (if a message is configured):
  - To disconnect the call, click **Disconnect Call**.
  - To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is `<username>@<domainName>` (for example, bob@contoso.com).

- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is `<username>@<domainName>`.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is `<number>@<domainName>` (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

24. Under **Step 5 Specify Your Holidays**, click the check boxes for one or more sets of holidays that define the days when the response group is closed for business.

**NOTE**

You need to define holidays and holiday sets before you configure the workflow. Use the **New-CsRgsHoliday** and **New-CsRgsHolidaySet** cmdlets to define holidays and holiday sets. For details, see [\(Optional\) Define Response Group holiday sets in Skype for Business](#).

25. If you want to play a message on holidays, select the **Play a message during holidays** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

**NOTE**

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

**NOTE**

All user-provided audio files must meet certain requirements. For details about supported audio file formats, see [Technical Requirements for Response Groups](#).

26. Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is `<username>@<domainName>` (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is `<username>@<domainName>`.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is `<number>@<domainName>` (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

27. Under **Step 6 Configure a Queue**, in **Select the queue that will receive the calls**, select the queue that you want to hold callers until an agent becomes available.

28. Under **Step 7 Configure Music on Hold**, choose the music you want callers to listen to while waiting for

an agent by doing one of the following:

- To use the default music-on-hold recording, click **Use default**.
- To use an audio file recording for the music on hold, click **Select a music file**. If you want to upload a new audio file, click the **a music file** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

**NOTE**

All user provided audio files must meet certain requirements. For details about supported audio file formats, see [Technical Requirements for Response Groups](#).

29. Click **Deploy**.

**To use Skype for Business Server Management Shell to create or modify a hunt group workflow**

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Create the prompt to be played for the welcome message, and save it in a variable. At the command line, run:

```
$promptWM = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>"
```

For example:

```
$promptWM = New-CsRgsPrompt -TextToSpeechPrompt "Welcome to Contoso. Please wait for an available agent."
```

**NOTE**

To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see [Import-CsRgsAudioFile](#).

4. Get the identity of the queue or question where the calls will be directed. At the command line, run:

```
$qid = (Get-CsRgsQueue -Name "Help Desk").Identity
```

For details about creating the queue, see [New-CsRgsQueue](#).

5. Define the default action to be taken when a workflow is opened during business hours, and save it in a variable. At the command line, run:

```
$actionWM = New-CsRgsCallAction -Prompt <saved prompt from previous step> -Action <action to be taken> -QueueID $qid
```

**NOTE**

For hunt group workflows, the default action must direct the call to a queue. This parameter is required for active workflows. It is not required for inactive workflows.

For example:

```
$actionWM = New-CsRgsCallAction -Prompt $promptWM -Action TransferToQueue -QueueID $qid.Identity
```

6. If you want to define business hours and holidays, you need to create them before you create or modify the workflow. For details, see [\(Optional\) Define Response Group business hours in Skype for Business](#) and [\(Optional\) Define Response Group holiday sets in Skype for Business](#).
7. If you want to have prompts for calls that are received out of business hours or on holidays, use the **New-CsRgsPrompt** cmdlet to define the prompt, and use the **New-CsRgsCallAction** to define the action to be taken after the prompt. For details, see [New-CsRgsPrompt](#) and [New-CsRgsCallAction](#).
8. Retrieve the service name for the Lync Server Response Group service and assign it to a variable. At the command, run:

```
$serviceId = "service:" + (Get-CsService | ?{$_ .Applications -like "*RGS*"}).ServiceId;
```

9. Create or modify the workflow. To create a workflow, use **New-CsRgsWorkflow**. To modify a workflow, use **Set-CsRgsWorkflow**. At the command line, type:

```
$workflowHG = New-CsRgsWorkflow -Parent <service ID for the Response Group service> -Name "<hunt group name>" [-Description "<hunt group description>"] -PrimaryUri "<SIP address for the workflow>" [-LineUri "<Phone number for the workflow>"] [-DisplayNumber "<Phone number displayed in Lync>"] [-Active <$true | $false>] [-Anonymous <$true | $false>] [-DefaultAction <variable from preceding step>] [-EnabledForFederation <$true | $false>] [-Managed <$true | $false>] [-ManagersByUri <SIP addresses for Response Group Managers who can manage the workflow>]
```

For example:

```
$workflowHG = New-CsRgsWorkflow -Parent $serviceID -Name "Human Resources" -Description "Human Resources workflow" -PrimaryUri "sip:humanresources@contoso.com" -LineUri "TEL:+14255551219" -DisplayNumber "555-1219" -Active $true -Anonymous $true -DefaultAction $actionWM -EnabledForFederation $false -Managed $true -ManagersByUri "sip:bob@contoso.com", "mindy@contoso.com"
```

#### IMPORTANT

All users who are designated managers for workflows must be assigned the CsResponseGroupManager role.

#### NOTE

For details about additional optional parameters, see [New-CsRgsWorkflow](#) or [Set-CsRgsWorkflow](#)

## Designing an interactive workflow

You can use interactive voice response (IVR) to obtain information from callers and direct the call to the appropriate queue. Question-and-answer pairs determine which queue to use. Depending on the caller's response, the caller either hears a follow-up question, or is routed to the appropriate queue. The IVR questions and the caller's responses are provided to the responding agent who accepts the call, providing valuable information to the agent.

### Overview of IVR Features

The Response Group application offers speech recognition and text-to-speech capabilities in 26 languages. You



can enter IVR questions using text-to-speech or a wave (.wav) or Windows Media audio (.wma) file. Callers can respond by using voice or dual-tone multifrequency (DTMF) responses.

Interactive workflows support up to two levels of questions, with each question having up to four possible answers. The IVR asks the caller a question, and depending on the caller's response, routes the caller to a queue or asks a second question. The second question can also have four possible answers. Depending on the answer to the second-level question, the caller is routed to the appropriate queue.

#### NOTE

When you design call flows by using Skype for Business Server Management Shell, you can define any number of levels of IVR questions and any number of answers. However, for caller usability, we recommend that you not use more than three levels of questions, with not more than five answers each. In addition, if you design a call flow that has more than two levels of questions with more than four answers each, you cannot edit the call flow by using Skype for Business Server Control Panel.

The IVR questions and the caller's responses are provided to the responding agent who accepts the call.

### Working with Speech Technologies

Speech technologies, such as speech recognition and text-to-speech, can enhance customer experience and let people access information more naturally and effectively. However, there can be cases where the specified text or the user voice response is not recognized correctly by the speech engine. For example, the "#" symbol is translated by the text-to-speech engine as the word "number." This issue can be mitigated by the following:

- The speech engine gives the caller five attempts to answer the question. If the caller answers the question incorrectly (that is, the answer is not one of the specified responses) or does not provide an answer at all, the caller gets another chance to answer the question. The caller has five attempts to answer the question before being disconnected. You can configure the IVR to play a customized message after each caller error. The question is repeated each time.
- To minimize the potential for ambient noise to be interpreted by the speech engine as a response, use longer responses. For example, responses should have more than one syllable and should sound significantly different from each other.
- If your questions have both speech and DTMF responses, configure the speech responses with words that represent the concept rather than the DTMF response. For example, instead of using "Press or say one" use "Press 1 or say billing."
- After you design your IVR, call the workflow, listen to the prompts, respond to each of the prompts using voice, and verify that the IVR sounds and behaves as expected. You can then modify the IVR to fix any interpretation issues. Following the previous example, if you need to refer to the # key, you can rewrite your IVR prompt to use the key name, rather than the # symbol. For example, "To talk to sales, press the pound key."

### IVR Design Examples

The following sections contain examples of different IVR scenarios and question-and-answer pairs.

#### IVR with One Level of Questions

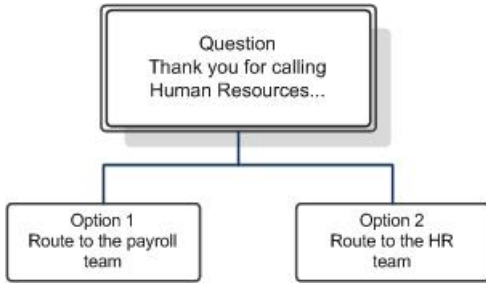
The following example shows an IVR that uses one level of questions. It uses speech recognition to detect the caller's response.

**Question:** "Thank you for calling Human Resources. If you would like to speak to payroll, say payroll. Otherwise, say HR."

- **Option 1 is selected:** The caller is routed to the payroll team.
- **Option 2 is selected:** The caller is routed to the human resources team.

The following figure shows the call flow.

### One-level interactive call flow



### IVR with Two Levels of Questions

The following example shows an IVR that uses two levels of questions. It allows callers to respond using either speech or DTMF keypad input.

**Question:** "Thank you for calling the IT Help Desk. If you have a network access problem, press 1 or say network. If you have a software problem, press 2 or say software. If you have a hardware problem, press 3 or say hardware."

- **Option 1 is selected:** The caller is routed to the network support team.
- **Option 2 is selected:** The caller is asked a follow-up question:

**Question:** "If this is an operating system problem, press 1 or say operating system. If this is a problem with an internal application, press 2 or say internal application. Otherwise, press 3 or say other."

- **Option 1 is selected:** The caller is routed to the operating systems support team.
- **Option 2 is selected:** The caller is routed to the internal applications support team.
- **Option 3 is selected:** The caller is routed to the software support team.

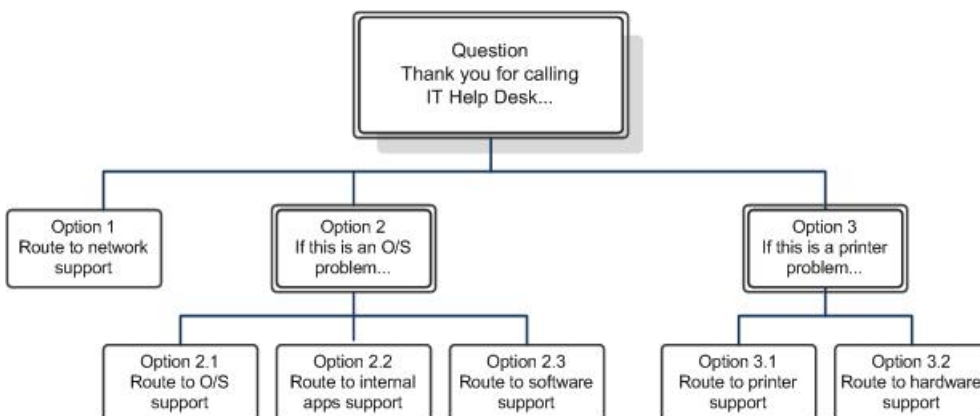
- **Option 3 is selected:** The caller is asked a follow-up question:

**Question:** "If this is a printer problem press 1. Otherwise, press 2."

- **Option 1 is selected:** The caller is routed to the printer support team.
- **Option 2 is selected:** The caller is routed to the hardware support team.

The following figure shows the call flow.

### Two-level interactive call flow



### Best Practices

The following list describes some best practices for designing your IVR:

- Let the caller get to the task quickly. Avoid providing too much information or lengthy marketing messages in your IVR.
- If you want to include a lengthy message, consider appending it to the first question instead of to the welcome message. Callers can bypass the message if it is part of the first question by answering the question, but they cannot bypass the welcome message.
- Speak in the caller's language. Avoid stilted language. Speak naturally.
- Write efficient and effective prompts. Remove any unnecessary options. Structure the information so that the caller's expected response is at the end of the sentence. For example, "To speak to the sales team, press 1."
- Make voice responses user friendly. For example, if you specify both DTMF and voice responses, use something like: "To speak to the sales team, press 1 or say sales."
- Test the IVR on a group of users before you deploy it across your organization.

## Creating or modifying an interactive workflow

### To use Response Group Configuration Tool to create or modify an Interactive workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service that hosts the workflow that you want to create or modify. In the resulting list of services, click the service that you want, and then click **OK**.

#### NOTE

The Response Group Configuration Tool opens. You can also open the Response Group Configuration Tool directly from a web browser by typing the following URL: `https://<webPoolFqdn>/RgsConfig`.

6. Do one of the following:
  - Under **Create a New Workflow**, next to **Interactive**, click **Create**.
  - Under **Manage an Existing Workflow**, locate the workflow you want to change, and then under **Action**, click **Edit**.
7. If you are not ready for users to start calling the workflow, clear the **Activate the workflow** check box.

#### NOTE

If you are creating a managed workflow, you need to select **Activate the workflow**. After you save the active, managed workflow, you can then modify and deactivate it.

8. To allow federated users to call the group, select the **Enable for federation** check box. You must also have an external access policy that applies to the Response Group application configured for federation.

**NOTE**

The global external access policy applies to the Response Group application. You can configure the global policy for response group federation by using Skype for Business Server Control Panel or by using the **Set-CsExternalAccessPolicy** cmdlet to set the EnableOutsideAccess parameter to True. Keep in mind that global policy settings apply to all users unless they are assigned a site or user policy. Therefore, before changing this setting for response groups, make sure that the federation setting meets the requirements of your organization. For details about how policies apply to users, see [Manage External Access Policy for Your Organization](#). For details about the federation setting, see **Set-CsExternalAccessPolicy** in documentation..

**NOTE**

Users who are hosted in Skype for Business Online can't place calls to response groups that are hosted in an on-premises deployment. This is true in both hybrid deployments and in cases where an on-premises deployment is federated with a Skype for Business Online deployment.

9. To hide the identity of agents during calls, select the **Enable agent anonymity** check box.

**NOTE**

Anonymous calls cannot start with instant messaging (IM) or video, although the agent or the caller can add IM and video after the call is established. An anonymous agent can also put calls on hold, transfer calls (both blind and consultative transfers), and park and retrieve calls. Anonymous calls do not support conferencing, application sharing and desktop sharing, file transfer, whiteboarding and data collaboration, and call recording. Agents using the Lync VDI Plugin can receive incoming calls anonymously, but they cannot make outgoing calls anonymously.

10. Under **Enter the address of the group that will receive the calls**, type the primary SIP uniform resource identifier (URI) address of the group that will answer calls to the workflow.
11. In **Display name**, type the name that you want to display for the workflow (for example, Sales IVR Response Group).

**NOTE**

Do not include the "<" or ">" characters in the display name. Do not use the following display names because they are reserved: **RGS Presence Watcher** or **Announcement Service**.

12. In **Telephone number**, type the line URI for the response group (for example, +14255550165).
13. In **Display number**, type the number as you want it to appear for the response group (for example, +1 (425) 555-0165).
14. (Optional) In **Description**, type a description for the workflow that you want to appear on the contact card in Skype for Business.
15. In **Workflow Type**, select **Managed** if this workflow will be managed by a Response Group Manager. Do the following to assign Response Group Managers to the workflow:
  - a. Type the SIP URI of a manager for this workflow, and click **Add**.
  - b. Type the SIP URI of additional managers to add to the workflow, and click **Add**.

### IMPORTANT

Every user who is designated as a manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

16. Under **Step 2 Select a Language**, click the language to use for speech recognition and text-to-speech.
17. If you want to configure a welcome message, under **Step 3 Configure a Welcome Message**, select the **Play a welcome message** check box, and then do one of the following:
  - To enter the welcome message as text that is converted to speech for callers, click **Use text-to-speech**, and then type the welcome message in the text box.

### NOTE

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use a Wave or Windows Media Audio file recording for the welcome message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the audio file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

### NOTE

All user-provided audio files must meet certain requirements. For details about supported file formats, see [Technical Requirements for Response Groups](#).

18. Under **Step 4 Specify Your Business Hours**, in the **Your time zone** box, click the time zone of the workflow.

### NOTE

The time zone is the time zone where the callers and agents of the workflow reside. It is used to calculate the open and close hours. For example, if the workflow is configured to use the North American Eastern Time zone and the workflow is scheduled to open at 7:00 A.M. and close at 11:00 P.M., the open and close times are assumed to be 7:00 Eastern Time and 11:00 Eastern Time respectively. (You must enter the times in 24-hour time notation.)

19. Select the type of business hours schedule you want to use by doing one of the following:
  - To use a predefined schedule of business hours, click **Use a preset schedule**, and then select the schedule you want to use from the drop-down list.

### NOTE

You must have defined at least one preset schedule previously to be able to select this option. You define preset schedules by using the **New-CsRgsHoursOfBusiness** cmdlet. For details, see [\(Optional\) Define Response Group business hours in Skype for Business](#). When you select a preset schedule, **Day**, **Open**, and **Close** are automatically filled with the days and hours that the response group is available.

- To use a custom schedule that applies only to this workflow, click **Use a custom schedule**.
20. If you are creating a custom schedule for this workflow, click the check boxes for the days of the week that the response group is available.

21. If you are creating a custom schedule, type the **Open** and **Close** hours when the response group will be available.

**NOTE**

The **Open** and **Close** hours must be in 24-hour time notation. For example, if your office works a 9-to-5 work day and closes at noon for lunch, the business hours are specified as **Open** 9:00, **Close** 12:00, **Open** 13:00, and **Close** 17:00.

22. If you want to play a message when the office is not open, select the **Play a message when the response group is outside of business hours** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

**NOTE**

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

**NOTE**

All user-provided audio files must meet certain requirements. For details about supported file formats, see [Technical Requirements for Response Groups](#).

23. Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is `<username>@<domainname>` (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is `<username>@<domainname>`.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is `<number>@<domainname>` (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

24. Under **Step 5 Specify Your Holidays**, click the check boxes for one or more sets of holidays that define the days when the response group is closed for business.

**NOTE**

You need to define holidays and holiday sets before you configure the workflow. Use the **New-CsRgsHoliday** and **New-CsRgsHolidaySet** cmdlets to define holidays and holiday sets. For details, see [\(Optional\) Define Response Group holiday sets in Skype for Business](#).

25. If you want to play a message on holidays, select the **Play a message during holidays** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

**NOTE**

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

**NOTE**

All user-provided audio files must meet certain requirements. For details about supported audio file formats, see [Technical Requirements for Response Groups](#).

26. Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is `<username>@<domainname>` (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is `<username>@<domainname>`.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is `<number>@<domainname>` (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

27. Under **Step 6 Configure Music on Hold**, choose what you want callers to listen to while waiting for an agent by doing one of the following:

- To use the default music on-hold recording, click **Use default**.
- To use an audio file recording for the on-hold music, click **Select a music file**. If you want to upload a new audio file, click the **a music file** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

**NOTE**

All user-provided audio files must meet certain requirements. For details about supported file formats, see [Technical Requirements for Response Groups](#).

28. Under **Step 7 Configure Interactive Voice Response**, under the **The user will hear the following text or recorded message** heading, specify the question to ask callers as follows:

- To enter the question in text format, click **Use text-to-speech**, and type the question in the text box.

**NOTE**

Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

**NOTE**

The "#" symbol is translated by the text-to-speech engine as the word "number". If you need to refer to the # key, you should use the key name, rather than the symbol, in your prompt. For example, "To talk to sales, press the pound key."

- To use a prerecorded audio file that contains the question, click **Select a recording**, and then click the **a recording** link to upload the file. In the new browser window, click **Browse**, select the audio file, and then click **Open**. Click **Upload** to load the file, and then optionally you can type the question in the text box (this enables the question, and the caller's response, to be forwarded to the responding agent).

**NOTE**

All user-provided audio files must meet certain requirements. For details about supported file formats, see [Technical Requirements for Response Groups](#).

29. Under **Response 1**, specify the first possible answer to the question by doing the following:

**IMPORTANT**

Do not use quotation marks (") in any voice responses. Quotation marks cause the IVR to fail.

**NOTE**

You can choose to allow callers to answer using speech, alphanumeric keypad input, or both.

- If you want to allow the caller to respond using speech, enter the answer in **Enter a voice response**.
  - If you want to allow the caller to respond by pressing a key on the keypad, in **Digit**, click the keypad digit.
30. Specify whether to route the caller to a queue, or to ask another question as follows:
- To route the caller to a queue, click **Send to a queue**, and in **Select a queue**, click the queue that you want to use.
  - To ask another question, click **Ask another question**, and then click **Use text-to-speech** and type the question, or click **Select a recording**. Use the response groupings in this section to specify up to four possible responses to the additional question and the queue to use for each response. To specify a third or fourth possible response, click the **Response 3** check box or the **Response 4** check box.
31. Specify up to three more possible answers to the original question by repeating steps 28 and 29 to specify the possible responses and the action to take for each response. To specify a third or fourth possible answer, click the **Response 3** check box or the **Response 4** check box.
32. Click **Deploy**.

**To use Skype for Business Server Management Shell to create or modify an Interactive workflow**



1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId = "service:" + (Get-CsService | ?{$_Applications -like "*RGS*"}).ServiceId;
```

4. An interactive workflow requires two or more queues and two or more agent groups. First, create the agent groups. Run:

```
$AGSupport = New-CsRgsAgentGroup -Parent $serviceId -Name "Technical Support" [-AgentAlertTime "20"] [-ParticipationPolicy "Informal"] [-RoutingMethod LongestIdle] [-AgentsByUri("sip:agent1@contoso.com", "sip:agent2@contoso.com")]  
$AGSales = New-CsRgsAgentGroup -Parent $serviceId -Name "Sales Team" [-AgentAlertTime "20"] [-ParticipationPolicy "Informal"] [-RoutingMethod LongestIdle] [-AgentsByUri("sip:bob@contoso.com", "sip:alice@contoso.com")]
```

5. Create the queues. Run:

```
$QSupport = New-CsRgsQueue -Parent $ServiceId -Name "Contoso Support" -AgentGroupIDList($AGSupport.Identity)  
$QSales = New-CsRgsQueue -Parent $ServiceId -Name "Contoso Sales" -AgentGroupIDList($AGSales.Identity)
```

6. Create the first response group prompt. Run:

```
$SupportPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Please be patient while we connect you with Contoso Technical Support."
```

7. Then create the action to be performed after the prompt. Run:

```
$SupportAction = New-CsRgsCallAction -Prompt $SupportPrompt -Action TransferToQueue -QueueID $QSupport.Identity
```

8. Create the first response group answer. Run:

```
$SupportAnswer = New-CsRgsAnswer -Action $SupportAction [-DtmfResponse 1]
```

9. Now create the second prompt, call action, and answer. First create the prompt. Run:

```
$SalesPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Please hold while we connect you with Contoso Sales."
```

10. Create the second call action. Run:

```
$SalesAction = New-CsRgsCallAction -Prompt $SalesPrompt -Action TransferToQueue -QueueID $QSales.Identity
```

11. Create the second response group answer. Run:

```
$SalesAnswer = New-CsRgsAnswer -Action $SalesAction [-DtmfResponse 2]
```

12. Create the top-level prompt. Run:

```
$TopLevelPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Thank you for calling Contoso. For Technical Support, press 1. For a Sales Representative, press 2."
```

13. Create the top-level question. Run:

```
$TopLevelQuestion = New-CsRgsQuestion -Prompt $TopLevelPrompt [-AnswerList ($SupportAnswer, $SalesAnswer)]
```

14. Now create the workflow. Run:

```
$IVRAction = New-CsRgsCallAction -Action TransferToQuestion [-Question $Question]  
$IVRWorkflow = New-CsRgsWorkflow -Parent $ServiceId -Name "Contoso Helpdesk" [-Description "The Contoso Helpdesk line."] -PrimaryUri "sip:helpdesk@contoso.com" [-LineUri tel:+14255554321] [-DisplayNumber "+1 (425) 555-4321"] [-Active $true] [-Anonymous $true] [-DefaultAction $IVRAction] [-Managed $true] [-ManagersByURI ("sip:mindy@contoso.com", "sip:bob@contoso.com")]
```

#### **NOTE**

All users who have been designated as manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

## See also

[\(Optional\) Define Response Group holiday sets in Skype for Business](#)

[\(Optional\) Define Response Group business hours in Skype for Business](#)

[New-CsRgsWorkflow](#)

[Set-CsRgsWorkflow](#)

[New-CsRgsPrompt](#)

[New-CsRgsCallAction](#)

# Managing application-level Response Group settings in Skype for Business

8/7/2019 • 2 minutes to read

Managing application-level Response Group settings, such as music-on-hold and ringback settings, in Skype for Business Server Enterprise Voice.

Application-level settings for Response Group application include the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration. You can define only one set of application-level settings per pool. To view application-level settings, use the **Get-CsRgsConfiguration** cmdlet. To modify the application-level settings, use the **Set-CsRgsConfiguration** cmdlet.

The default music on hold is played when a call is placed on hold only if no custom music on hold is defined. Call context is available only for queues assigned to interactive workflows. If call context is enabled, an agent can see information such as caller wait time or workflow questions and answers when the call is received.

## To modify Response Group application-level settings

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. At the command line, run:

```
Set-CsRgsConfiguration -Identity <name of service hosting Response Group> [-AgentRingbackGracePeriod <# seconds until call returns to agent after declined>] [-DefaultMusicOnHoldFile <audio file>] [-DisableCallContext <$true | $false>]
```

For example:

```
Set-CsRgsConfiguration -Identity "service:ApplicationServer:redmond.contoso.com" -AgentRingbackGracePeriod 30 -DisableCallContext $false
```

To specify an audio file to use as the default music on hold, you need to import the audio file first. For example:

```
$x = Import-CsRgsAudioFile -Identity "service:ApplicationServer:redmond.contoso.com" -FileName "MusicWhileYouWait.wav" -Content (Get-Content C:\Media\MusicWhileYouWait.wav -Encoding byte -ReadCount 0)
Set-CsRgsConfiguration -Identity "service:ApplicationServer:redmond.contoso.com" -DefaultMusicOnHoldFile <$x>
```

## See also

[Get-CsRgsConfiguration](#)

[Set-CsRgsConfiguration](#)

[Import-CsRgsAudioFile](#)

# (Optional) Verify Response Group deployment in Skype for Business

8/7/2019 • 2 minutes to read

Verify your Response Group deployment success, in Skype for Business Server Enterprise Voice.

After you configure Response Group, you need to verify the configuration to make sure your response groups work as expected. At minimum, verify the following scenarios by using the following types of users:

## Users

- A user who is homed on Skype for Business
- An external user who uses the public switched telephone network (PSTN)
- An agent who is homed on Skype for Business

## Scenarios

- The Skype for Business user calls the response group.
- The external user calls the response group.
- A user calls the response group while the agent is on another call and goes to the queue.

### NOTE

If the response group does not work as expected please check next link: <https://support.office.com/en-us/article/troubleshooting-for-response-groups-ca72d8f8-4054-4974-b832-4f173611bd89>

# Deployment process for the Announcement application in Skype for Business Server

8/7/2019 • 2 minutes to read

Deployment process and steps for Announcement application in Skype for Business Server Enterprise Voice.

The Announcement application is an Enterprise Voice feature that enables you to configure what happens to calls to unassigned extensions (extensions that are valid for your organization, but are not assigned to a person or a phone). For example, you can configure calls to unassigned numbers to play a message, or to be transferred to a different destination, or both.

The Announcement application is installed as a feature of Response Group application on the Front End Server or Standard Edition server when you deploy Enterprise Voice. You need to configure Announcements by uploading your audio files or by configuring text-to-speech (TTS) and configuring the unassigned number table.

This section provides an overview of the steps involved in deploying the Announcement application. You must deploy Enterprise Voice before you configure announcements. The components required by the Announcement application are installed and enabled when you deploy Enterprise Voice.

## Announcement Deployment Process

PHASE	STEPS	ROLES	DEPLOYMENT DOCUMENTATION
Configure Announcement settings	Create the announcement by recording and uploading audio files or by using text-to-speech (TTS). Configure the unassigned number ranges in the unassigned number table and associate them with the appropriate announcement.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator CsViewOnlyAdministrator	<a href="#">Create or delete an announcement in Skype for Business Server</a> <a href="#">Create or modify an unassigned number range in Skype for Business Server</a>
Verify your Announcement deployment	Test by listening to announcements to verify that your configuration works as expected.	-	<a href="#">(Optional) Verify Announcement deployment in Skype for Business</a>

# Create or delete an announcement in Skype for Business Server

8/7/2019 • 3 minutes to read

Create or delete announcements for Announcement application in Skype for Business Server Enterprise Voice. This affects how calls to unassigned numbers are handled.

When you configure announcements, you are really configuring how you want calls to unassigned numbers to be handled. You can play a prompt, which can be an audio file or a text-to-speech (TTS) file, or you can just transfer the call to a specified destination without playing a prompt.

You need to create announcements before you define the unassigned number table. You need to perform this step for all announcements that use an audio prompt, a TTS prompt, or no prompt.

This topic describes how to import and create announcements. For details about assigning announcements in the unassigned number table, see [Configure the Unassigned Number Table](#).

## Create a new announcement for unassigned numbers

To create a new announcement, you need to perform the following steps:

1. For audio prompts, record the audio file by using your favorite audio recording application.
2. For audio prompts, run the **Import-CsAnnouncementFile** cmdlet to import the contents of the audio file to File Store.
3. Run the **New-CsAnnouncement** cmdlet to create and name the announcement. Perform this step to create announcements with an audio prompt, a text-to-speech (TTS) prompt, or no prompt.

### TIP

You might want to create an announcement with no prompt (for example, if you want to transfer calls to a specific destination without playing a message).

4. Assign the new announcement to a number range in the unassigned number table.

### To create a new announcement

1. For audio prompts, create the audio file.
2. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
3. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
4. For audio prompts, run:

```
Import-CsAnnouncementFile -Parent <service of the Application Server running the Announcement application> -FileName <name for file in File Store> -Content Byte [<contents of file in byte array>]
```

5. Run:

```
New-CsAnnouncement -Parent <service of Application Server running the Announcement application, in the form: service:ApplicationServer:<fqdn>> -Name <unique name to be used as destination in unassigned number table> [-AudioFilePrompt <FileName specified in Import-CsAnnouncementFile>] [-TextToSpeechPrompt <text string to be converted to speech>] [-Language <Language for playing the TTS prompt (required for PromptTts)>] [-TargetUri sip:SIPAddress for transferring caller after announcement]
```

For transferring calls to voice mail, type SIPAddress in the format sip:username@domainname;opaque=app:voicemail (for example, sip:bob@contoso.com;opaque=app:voicemail). For transferring calls to a phone number, type SIPAddress in the format sip:number@domainname;user=phone (for example, sip:+14255550121@contoso.com;user=phone).

For example, to specify an audio prompt:

```
$a = Get-Content ".\PromptFile.wav" -ReadCount 0 -Encoding Byte
Import-CsAnnouncementFile -Parent service:ApplicationServer:pool0@contoso.com -FileName
"ChangedNumberMessage.wav" -Content $a
New-CsAnnouncement -Parent service:ApplicationServer:pool0.contoso.com -Name "Number Changed
Announcement" -AudioFilePrompt "ChangedNumberMessage.wav"
```

For example, to specify a TTS prompt:

```
New-CsAnnouncement -Parent service:ApplicationServer:pool0.contoso.com -Name "Help Desk Announcement" -
TextToSpeechPrompt "The Help Desk number has changed. Please dial 5550100." -Language "en-US"
```

For more detail about these cmdlets, and to see a list of the language codes to use in the **TextToSpeechPrompt** parameter, see [New-CsAnnouncement](#).

## Delete an announcement for unassigned numbers

### To delete an announcement

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. List all the announcements in your organization. At the command line, run:

```
Get-CsAnnouncement
```

4. In the resulting list, locate the announcement you want to delete, and copy the GUID. Then, at the command line, run:

```
Remove-CsAnnouncement -Identity "<Service:service ID/guid>"
```

For example:

```
Remove-CsAnnouncement -Identity "ApplicationServer:Redmond.contoso.com/1951f734-c80f-4fb2-965d-51807c792b90"
```

**NOTE**

For details about more options, see [Get-CsAnnouncement](#) and [Remove-CsAnnouncement](#).

## See also

[Create or delete an announcement in Skype for Business Server](#)

[Import-CsAnnouncementFile](#)

[New-CsAnnouncement](#)

[Remove-CsAnnouncement](#)

[Get-CsAnnouncement](#)



# Create or modify an unassigned number range in Skype for Business Server

8/7/2019 • 6 minutes to read

Create, modify or delete unassigned number ranges for Announcement application in Skype for Business Server Enterprise Voice. This affects how calls to unassigned numbers are handled.

Skype for Business Server enables you to say what happens to incoming calls to phone numbers that are valid for your organization, but are not assigned to a user or a phone. To handle such calls, you set up an unassigned number table. You can use the table to route the calls to an Announcement application or to an Exchange UM server.

How you configure the unassigned number table depends on how you want to use it. You can configure the table with all the valid extensions for your organization, with only unassigned extensions, or with a combination of both types of numbers. The unassigned number table can include both assigned and unassigned numbers, but it is invoked only when a caller dials a number that is not currently assigned. If you include all the valid extensions in the unassigned number table, you can specify the action that occurs whenever someone leaves your organization, without needing to reconfigure the table. If you include unassigned extensions in the table, you can modify the action that occurs for specific numbers. For example, if you change the extension for your customer service desk, you can include the old customer service number in the table and then assign it to an announcement that provides the new number.

## Configure unassigned phone numbers

Use one of the following procedures to configure unassigned number ranges for the Announcement application.

### IMPORTANT

Before you configure the unassigned number table, your system must already either have Announcements defined or an Exchange Unified Messaging (UM) Auto Attendant set up.

### TIP

When someone calls an unassigned number, Skype for Business Server searches the unassigned number table from top to bottom and uses the first matching range. Therefore, an action that you want to be performed as a last resort should be specified for the last range in the table.

### To use Skype for Business Server Control Panel to configure unassigned phone numbers

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice Features**, and then click **Unassigned Number**.
4. On the **Unassigned Number** page, do one of the following:
  - To create a new number range, click **New**. In **Name**, type an identifying name for this range of

numbers.

**NOTE**

After you commit the new unassigned number range to the database, you cannot change this name.

- To modify an existing number range, type all or part of the name of the number range in the search field. In the resulting list of number ranges, click the name you want, click **Edit**, and then click **Show details**.
5. In the first **Number range** field, type the beginning number of the range, and in the second **Number range** field, type the ending number of the range.
    - The beginning number of the range must be less than or equal to the ending number of the range.
    - If the beginning number of the range or the ending number of the range includes an extension number, both the beginning number and the ending number of the range must include an extension, and the extension number must be the same for both the beginning number and the ending number.
    - The number must match the regular expression (tel:)?(+)?[1-9]\d{0,17};ext=[1-9]\d{0,9}?. This means the number may begin with the string tel: (if you don't specify that string, it will be automatically added for you), a plus sign (+), and a digit 1 through 9. The phone number can be up to 17 digits and may be followed by an extension in the format ;ext= followed by the extension number.
  6. In **Announcement service**, do one of the following:
    - Click **Announcement**.
    - Click **Exchange UM**.
  7. If, in the previous step, you clicked **Announcement**, do the following:
    - a. Under **FQDN of destination server**, click **Select**, click the service ID of the Application service that runs the Announcement application that will handle incoming calls to this range of unassigned numbers, and then click **OK**.
    - b. In **Announcement**, click the announcement to be played for this range of unassigned numbers.
  8. If, in the previous step, you clicked **Exchange UM**, under **Auto Attendant phone number**, click **Select**, click the phone number to be used for this range of unassigned numbers, and then click **OK**.
  9. Click **OK**.
  10. On the **Unassigned Number** page, be sure that the unassigned number ranges are arranged in the order that you want. To change a range's position in the table, click one or more consecutive names in the list of ranges, and then click the up arrow or the down arrow.

**TIP**

Skype for Business Server searches the unassigned number table from top to bottom and uses the first range that matches the unassigned number. If you have overlapping ranges and one range specifies a last resort action, make sure that range is at the bottom of the list.

11. When you have the unassigned number ranges in the order that you want, click **Commit all**.

**To use Skype for Business Server Management Shell to configure unassigned phone numbers**

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup**

## Permissions.

2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Use **New-CsUnassignedNumber** to create a new unassigned number range. Use **Set-CsUnassignedNumber** to modify an existing unassigned number range.

### TIP

If you have overlapping ranges and want the ranges to be applied in a specific order, include the Priority parameter. The range with the highest priority will be applied to the call. The value 0 represents the highest priority.

At the command line, do one of the following:

- To create a number range for an Announcement service, run:

```
New-CsUnassignedNumber -Identity <unique identifier for unassigned number range> -  
NumberRangeStart <first number in range> -NumberRangeEnd <last number in range> -AnnouncementName  
<announcement name> -AnnouncementService <FQDN or service ID of the Announcement service>
```

- Or, to create a number range for Exchange UM Auto Attendant, run:

```
New-CsUnassignedNumber -ExUmAutoAttendantPhoneNumber <phone number> -Identity <unique identifier  
for unassigned number range> -NumberRangeStart <first number in range> -NumberRangeEnd <last  
number in range>
```

For example:

```
New-CsUnassignedNumber -Identity "Unassigned range 1" -NumberRangeStart "+14255551000" -  
NumberRangeEnd "+14255551100" -AnnouncementName "Welcome Announcement" -AnnouncementService  
ApplicationServer:Redmond.contoso.com
```

Or

```
New-CsUnassignedNumber -ExUmAutoAttendantPhoneNumber "+12065551234" -Identity "Unassigned range  
1" -NumberRangeStart "+14255551000" -NumberRangeEnd "+14255551100"
```

The following example shows how to modify the numbers in an existing unassigned number range:

```
Set-CsUnassignedNumber -Identity "Unassigned range 1" -NumberRangeStart "+14255551000" -  
NumberRangeEnd "+14255551900"
```

## Delete an unassigned number range

### To use Skype for Business Server Control Panel to delete an unassigned number range

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.

3. In the left navigation bar, click **Voice Features** and then click **Unassigned Number**.
4. On the **Unassigned Number** page, in the search field, type all or part of the name of the unassigned number range you want to delete.
5. In the resulting list of number ranges, click the name, click **Edit**, and then click **Delete**.
6. Click **Commit all**.

#### To use Skype for Business Server Management Shell to delete an unassigned number range

1. Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. At the command line, type:

```
Remove-CsUnassignedNumber -Identity "<name of unassigned number range>"
```

For example:

```
Remove-CsUnassignedNumber -Identity "Unassigned range 1"
```

#### NOTE

For details about more options, see [Remove-CsCallParkOrbit](#).

## See also

[New-CsUnassignedNumber](#)

[Set-CsUnassignedNumber](#)

[Get-CsUnassignedNumber](#)

# (Optional) Verify Announcement deployment in Skype for Business

8/7/2019 • 2 minutes to read

Verifying your deployment of Announcement application in Skype for Business Server Enterprise Voice. This affects how calls to unassigned numbers are handled.

After you install and configure Announcement, you need to verify the configuration to make sure that calls to unassigned numbers work as expected. At minimum, verify the following:

- Call a number that is valid for your organization but is an unassigned number.
- Call the unassigned number and verify that the correct announcement plays.

# Deploy Shared Line Appearance in Skype for Business Server 2015

11/1/2019 • 3 minutes to read

Read this topic to learn how to deploy Shared Line Appearance (SLA) in Skype for Business Server 2015, November 2015 Cumulative Update. SLA is a feature for handling multiple calls on a specific number called a shared number.

For more information about this feature, see [Plan for Shared Line Appearance in Skype for Business Server 2015](#).

Shared Line Appearance (SLA) is a new feature in Skype for Business Server, November 2015 Cumulative Update. To enable this feature, you must have first deployed this cumulative update.

## Install Shared Line Appearance

1. After Skype for Business Server, November 2015 Cumulative Update is deployed, run the `SkypeServerUpdateInstaller.exe` patch on each Front End Server in the pool.
2. The installer will deploy the latest version of the SLA application, however, the application is not enabled by default. It is enabled by following the steps outlined below:
  - a. Register SLA as a server application by running the following command for each pool:

```
New-CsServerApplication -Identity 'Service:Registrar:%FQDN%/SharedLineAppearance' -Uri http://www.microsoft.com/LCS/SharedLineAppearance -Critical $false -Enabled $true -Priority (Get-CsServerApplication -Identity 'Service:Registrar:%FQDN%/UserServices').Priority
```

where %FQDN% is the fully qualified domain name of the pool.

- b. Run the following command to update the RBAC roles for the SLA cmdlets:

```
Update-CsAdminRole
```

- c. Restart all the Front End Servers (RTCSRVR service) in all the pools where SLA was installed and enabled:

```
Stop-CsWindowsService RTCSRVR Start-CsWindowsService RTCSRVR
```

## Create an SLA group and add users to it

1. Create the SLA group by using the `Set-CsSlaConfiguration` cmdlet:

```
Set-CsSlaConfiguration -Identity <IdentityOfGroup> -MaxNumberOfCalls <Number> -BusyOption <BusyOnBusy|Voicemail|Forward> [-Target <TargetUserOrPhoneNumber>]
```

The `Set-CsSlaConfiguration` cmdlet marks the Enterprise Voice account `SLAGroup1` as an SLA entity, and the number of `SLAGroup1` becomes the number for the SLA group. All calls to `SLAGroup1` will ring the entire SLA group.

The following example creates an SLA group for an existing Enterprise Voice user, `SLAGroup1`, and uses the number assigned for `SLAGroup1` as the SLA mainline number.

The command sets the maximum number of concurrent calls for the new SLA group to 3, and for calls in

excess of that to hear a busy signal:

```
Set-CsSlaConfiguration -Identity SLAGroup1 -MaxNumberOfCalls 3 -BusyOption BusyOnBusy
```

You can use `Set-CsSlaConfiguration` to create a new SLA group or modify an existing one.

#### NOTE

Note that what you specify for `-Identity` must be a valid existing Enterprise Voice-enabled user account.

2. Add delegates to the group by using the `Add-CsSlaDelegates` cmdlet:

```
Add-CsSlaDelegates -Identity <IdentityOfGroup> -Delegate  
<NameOfDelegate@domain>
```

The following example adds a user to the SLA group. Each user added to the group must be a valid Enterprise Voice-enabled user:

```
Add-CsSlaDelegates -Identity SLAGroup1 -Delegate sip:SLA_Delegate1@contoso.com
```

Repeat the cmdlet for each user you want to add to the group. Users can only belong to a single SLA group.

### Configure the SLA group Busy Option

- Configure the SLA group Busy Option by using the `Set-CsSlaConfiguration` cmdlet:

```
Set-CsSlaConfiguration -Identity <IdentityOfGroup> -BusyOption <Option> [-Target  
<TargetUserOrPhoneNumber>]
```

The following example sets calls that exceed the maximum number of concurrent calls to be forwarded to the telephone number 202-555-1234. The target could be a user in your organization instead of a phone number; in that case, the syntax for the person to receive the forwarded calls is the same as when you specify a delegate: `sip:<NameOfDelegate@domain>`. The other possible parameter for `BusyOption` is `Voicemail`:

```
Set-CsSlaConfiguration -Identity SLAGroup1 -BusyOption Forward -Target tel:+2025551234
```

### Configure the SLA group Missed Call Option

1. Configure the SLA group Missed Call Option by using the `Set-CsSlaConfiguration` cmdlet:

```
Set-CsSlaConfiguration -Identity <IdentityOfGroup> -MissedCallOption <Option> -MissedCallForwardTarget  
<TargetUserOrPhoneNumber> -BusyOption <Option> -MaxNumberOfCalls <#> -Target [Target]
```

2. The following example specifies that missed calls are to be forwarded to the user named `sla_forward_number`. The valid options for the `-MissedCallOption` parameter are `Forward`, `BusySignal`, or `Disconnect`. If you choose `Forward`, you must also include the `-MissedCallForwardTarget` parameter, with a user or phone number as the target:

```
Set-CsSlaConfiguration -Identity SLAGroup1 -MissedCallOption Forward -MissedCallForwardTarget
sip:sla_forward_number@contoso.com -BusyOption Forward -MaxNumberOfCalls 2 -Target
sip:sla_forward_number@contoso.com
```

### Remove a delegate from a group

- Remove a delegate from a group by using the [Remove-CsSlaDelegates](#) cmdlet:

```
Remove-CsSlaDelegates -Identity <IdentityOfGroup> -Delegate <NameOfDelegate@domain>
```

For example:

```
Remove-CsSlaDelegates -Identity SLAGroup1 -Delegate sip:SLA_Delegate3@contoso.com
```

### Delete an SLA group

- Delete an SLA group by using the [Remove-CsSlaConfiguration](#) cmdlet:

```
Remove-CsSlaConfiguration -Identity <IdentityOfGroup>
```

For example:

```
Remove-CsSlaConfiguration -Identity SLAGroup1
```



# Install and configure Busy Options for Skype for Business Server

8/7/2019 • 4 minutes to read

Read about how to install and configure Busy Options in Skype for Business Server.

Busy Options is a new voice policy introduced in the July 2016 Cumulative Update that allows you to configure how incoming calls are handled when a user is already in a call or conference or has a call placed on hold. New or incoming calls can be rejected with a busy signal or forwarded to voice mail.

If Busy Options is enabled for the organization, all users at the Enterprise, both Enterprise Voice and non-Enterprise Voice users, can use the following configuration options:

- Busy on Busy - In which new incoming calls will be rejected with a busy signal if the user is busy.
- Voicemail on Busy - In which new incoming calls will be forwarded to voice mail if the user is busy.

Regardless of how their busy options are configured, users in a call or conference, or those with a call on hold, are not prevented from initiating new calls or conferences.

For more information about the Busy Options feature, see [Plan for Busy Options for Skype for Business Server](#).

## Install

Make sure you have the latest version of Skype for Business Server installed and that you have installed the most recent patch. To do this, first stop all services, and then run the Skype for Business Server update installer as follows:

1. Run the Stop-CsWindowsService command.
2. Run the SkypeServerUpdateInstaller.exe installer on each Front End server in a pool.
3. Run the SkypeServerUpdateInstaller.exe installer on each Survivable Branch Server (SBS), if you want to ensure support for failover on SBS.

The installer will deploy the latest version of the Busy Options application. However, the application is not enabled by default. To enable the application, perform the following steps:

1. Run the [Set-CsVoicePolicy](#) cmdlet to globally enable Busy Options as shown in the following example:

```
Set-CsVoicePolicy -EnableBusyOptions $true
```

2. Next, if the site has a voice policy in place, you must enable Busy Options for the voice policy as follows:

First, run [Get-CsSite](#) to retrieve the name of the site:

```
Get-CsSite
```

Use the Identity value (for example: Site:Redmond1) retrieved from Get-CsSite to retrieve the voice policy of the site as follows:

```
Get-CsVoicePolicy -Identity Site:Redmond1
```

If a voice policy exists for the site, run the following command:

```
Set-CsVoicePolicy -Identity Site:Redmond1 -EnableBusyOptions $true
```

- Next, run the [New-CsServerApplication](#) cmdlet to add Busy Options to the list of server applications as shown in the following example:

```
New-CsServerApplication -Identity 'Service:Registrar:%FQDN%/BusyOptions' -Uri  
http://www.microsoft.com/LCS/BusyOptions -Critical $False -Enabled $True -Priority (Get-  
CsServerApplication -Identity 'Service:Registrar:%FQDN%/UserServices').Priority
```

#### NOTE

You must replace %FQDN% with the fully-qualified domain name of a specific pool.

- Next, run the [Update-CsAdminRole](#) cmdlet to update the Role-based access control (RBAC) roles for the Busy Options cmdlets as shown in the following example:

```
Update-CsAdminRole
```

- Finally, start the Skype for Business Server Windows services on all the Front End servers in all the pools where Busy Options was installed and enabled by running the [Start-CsWindowsService](#) command:

```
Start-CsWindowsService
```

## Configure

To configure Busy Options, use the [Set-CsBusyOptions](#) cmdlet.

For example, the following command configures busy options for the user "Ken Myer". In this configuration, any call to "Ken Myer" will return a busy signal when he is already in a call:

```
Set-CsBusyOptions -Identity "Ken Myer" -ActionType BusyOnBusy
```

In the next example, the command configures busy options for the user "Chrystal Velasquez". In this configuration, new incoming calls to "Chrystal Velasquez" will be forwarded to voice mail when she is already in a call:

```
Set-CsBusyOptions -Identity "Chrystal Velasquez" -ActionType VoicemailOnBusy
```

You can retrieve configuration information about Busy Options by using the [Get-CsBusyOptions](#) cmdlet. The following example returns the Busy Options setting for "KenMyer@Contoso.com":

```
Get-CsBusyOptions -Identity sip:KenMyer@Contoso.com
```

You can remove Busy Options by using the [Remove-CsBusyOptions](#) cmdlet. The following command removes Busy Options for "Ken Myer":

```
Remove-CsBusyOptions -Identity "Ken Myer"
```

For detailed information about the cmdlets you use to configure Busy Options, see the technical reference content for [Set-CsBusyOptions](#), [Get-CsBusyOptions](#), and [Remove-CsBusyOptions](#).

## Enable logging

To enable logging for Busy Options by using the Centralized Logging Service, specify the following:

```
$p1 = New-CsClsProvider -Name S4 -Type WPP -Level Info -Flags All
$p2 = New-CsClsProvider -Name Sipstack -Type WPP -Level Info -Flags
      "TF_PROTOCOL,TF_CONNECTION,TF_SECURITY,TF_DIAG,TF_SHOW_CONFERENCE,TF_SHOW_ALLREQUESTS,TF_SHOW_ALLSIPHEADERS"
-Role Registrar
$p3 = New-CsClsProvider -Name BusyOptions -Type WPP -Level Verbose -Flags All
New-CsClsScenario -Parent Global -Name BusyOptions -Provider @{Add=$p1,$p2,$p3}
```

## Verify and troubleshoot

After installing Busy Options, you can verify that the installation was successful by using the [Get-CsServerApplication](#) cmdlet to retrieve the list of server applications. If Busy Options is installed properly, the output of the cmdlet should show the Busy Options configuration as follows:

```
Identity   : Service:Registrar:pool0.vdomain.com/BusyOptions
Priority    : 5
Uri         : http://www.microsoft.com/LCS/BusyOptions
Name       : BusyOptions
Enabled    : True
Critical   : False
ScriptName :
Script     :
```

You can also use Windows Event Viewer to verify that the Busy Options installation was successful and that Skype for Business Server successfully loaded Busy Options. To verify Busy Options, open **Event Viewer -> Application and Services Logs -> Skype (or Lync) Server** and search for Event ID = 30253.

# Integrate Skype for Business Server with Exchange Server

8/7/2019 • 2 minutes to read

**Summary:** Review integration steps for Exchange Server 2013 or later and Skype for Business Server.

Exchange Server 2013 or later and Skype for Business Server are compatible and integrate well. For example, Skype for Business user presence information can be reported in Microsoft Outlook; likewise, Skype for Business can access a user's Outlook calendar, notice the user has a meeting scheduled, and show the user's presence as Busy during the meeting. Although you do not have to run Exchange Server in order to run Skype for Business Server (or vice-versa) the two products together enhance each other's user experience.

This documentation provides information on integrating Skype for Business Server and Exchange Server 2016 or Exchange Server 2013, but it assumes the initial setup and configuration of these two products has already happened. For details about deploying Skype for Business Server see the [Skype for Business Server Tech Center](#). For details about deploying Exchange Server see the deployment documentation for your version of Exchange.

If you are integrating an on premises installation of Skype for Business Server with Microsoft Exchange Online, see [Configure integration between on-premises Skype for Business Server and Outlook Web App](#).

If you are integrating Skype for Business Online with Exchange Server on premises, see [Configure OAuth between Skype for Business Online and Exchange on premises](#).

## In this section

[Configure partner applications in Skype for Business Server and Exchange Server](#)

[Configure Skype for Business Server to use Exchange Server archiving](#)

[Configure SharePoint Server to search for archived Skype for Business data](#)

[Configure Skype for Business Server to use the unified contact store](#)

[Configure the use of high-resolution photos in Skype for Business Server](#)

[Configure Exchange Server Unified Messaging for Skype for Business Server voice mail](#)

[Integrating Skype for Business Server and Microsoft Outlook Web App 2013](#)

[Configure the personal contacts store on client computers for Skype for Business Server](#)

## See also

[Plan to integrate Skype for Business and Exchange](#)

# Configure partner applications in Skype for Business Server and Exchange Server

8/7/2019 • 4 minutes to read

**Summary:** Configure server to server authentication for Exchange Server 2016 or Exchange Server 2013 and Skype for Business Server.

Server-to-server authentication usually requires two servers that need to communicate with one another and a third-party security token server. If Server A and Server B need to communicate, then both of those servers typically start by contacting a token server and obtaining a mutually-trusted security token. Server A then presents that security token to Server B (and vice-versa) as a way to guarantee its authenticity and trustworthiness.

However, that's a general rule. Skype for Business Server, Exchange Server 2016, Exchange Server 2013, and SharePoint Server 2013 do not need to use a third-party token server when communicating with one another; that's because these server products can create security tokens that can be accepted by one another without the need for a separate token server. (This capability is only available in Skype for Business Server, Exchange Server 2016, Exchange Server 2013, and SharePoint Server 2013. If you need to set up server-to-server authentication with other servers, including other Microsoft server products, then you will need to do so by using a third-party token server.)

In order to set up server-to-server authentication between Skype for Business Server and Exchange Server you must do two things: 1) you must assign the appropriate certificates to each server; and, 2) you must configure each server to be a partner application of the other server: that means you must configure Skype for Business Server to be a partner application for Exchange Server, and you must configure Exchange Server to be a partner application for Skype for Business Server.

## Configuring Skype for Business Server to be a Partner Application for Exchange Server

The easiest way to configure Skype for Business Server to be a partner application with Exchange Server 2016 or Exchange Server 2013 is to run the `Configure-EnterprisePartnerApplication.ps1` script, a Windows PowerShell script that ships with Exchange Server. To run this script, you must provide the URL for the Skype for Business Server authentication metadata document; this will typically be the fully qualified domain name of the Skype for Business Server pool followed by the suffix `/metadata/json/1`. For example:

```
https://atl-cs-001.litwareinc.com/metadata/json/1
```

To configure Skype for Business Server as a partner application, open the Exchange Management Shell and run a command similar to this (assuming that Exchange has been installed on drive C: and that it uses the default folder path):

```
"C:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartnerApplication.ps1 -AuthMetadataUrl 'https://atl-cs-001.litwareinc.com/metadata/json/1' -ApplicationType Lync"
```

After configuring the partner application it is recommended that you stop and restart Internet Information Services (IIS) on your Exchange mailbox and client access servers. You can restart IIS by using a command similar to this, which restarts the service on the computer `atl-exchange-001`:

```
iisreset atl-exchange-001
```

This command can be run from within the Exchange Management Shell or from any other command window run under administrator privileges.

## Configuring Exchange Server to be a Partner Application for Skype for Business Server

After you have configured Skype for Business Server to be a partner application for Exchange Server 2016 or Exchange Server 2013, you must then configure Exchange Server to be a partner application for Skype for Business Server. This can be done by using the Skype for Business Server Management Shell and specifying the authentication metadata document for Exchange; this will typically be the URI of the Exchange autodiscover service followed by the suffix `/metadata/json/1`. For example:

```
https://autodiscover.litwareinc.com/autodiscover/metadata/json/1
```

In Skype for Business Server, partner applications are configured by using the `New-CsPartnerApplication` cmdlet. In addition to specifying the metadata URI you should also set the application trust level to Full; this will allow Exchange to represent both itself and any authorized user in the realm. For example:

```
New-CsPartnerApplication -Identity Exchange -ApplicationTrustLevel Full -MetadataUrl  
"https://autodiscover.litwareinc.com/autodiscover/metadata/json/1"
```

Alternatively, you can create a partner application by copying and modifying the script code found in the Skype for Business Server server-to-server authentication documentation. See the [Manage server-to-server authentication \(OAuth\) and partner applications in Skype for Business Server](#) article for more information.

If you have successfully configured partner applications for both Skype for Business Server and Exchange Server, you have also successfully configured server-to-server authentication between the two products. Skype for Business Server includes a Windows PowerShell cmdlet, `Test-CsExStorageConnectivity` which enables you to verify that server-to-server authentication has been correctly configured and that the Skype for Business Server Storage Service can connect to Exchange Server. The cmdlet does this by connecting to the mailbox of an Exchange Server user, writing an item into the Conversation History folder for that user, and then (optionally) deleting that item.

To test the integration of Skype for Business Server and Exchange Server, run a command similar to the following from the Skype for Business Server Management Shell:

```
Test-CsExStorageConnectivity -SipUri "sip:kenmyer@litwareinc.com"
```

In the preceding command, the `SipUri` represents the SIP address of a user with an account on Exchange Server; your command will fail in this is not a valid user account.

### NOTE

If you receive a 401 response from this cmdlet, it is probably because the default configuration for Exchange does not include support for accepting OAuth tokens. For more information about using OAuth in Exchange, see [Configure OAuth authentication with SharePoint 2013 and Skype for Business Server](#).

If the test succeeds and connectivity has been established, you can then proceed to configure optional features such as archiving integration and the unified contact store.



# Configure Skype for Business Server to use Exchange Server archiving

8/7/2019 • 8 minutes to read

**Summary:** Configure IM transcripts for Exchange Server 2016 or Exchange Server 2013 and Skype for Business Server.

Skype for Business Server gives administrators the option of having instant messaging and Web conferencing transcripts archived to a user's Exchange Server 2016 or Exchange Server 2013 mailbox rather than a SQL Server database. If you enable this option, transcripts are written to the Purges folder in the user's mailbox. The Purges folder is a hidden folder found in the Recoverable Items folder. Although this folder is not visible to end users, the folder is indexed by the Exchange search engine and can be discovered by using Exchange mailbox search and/or Microsoft SharePoint Server 2013. Because information is stored in the same folder used by the Exchange In-Place Hold feature (responsible for archiving email and other Exchange communications), administrators can use a single tool to search for all the electronic communications archived for a user.

## IMPORTANT

To completely disable conversation archiving, you must also disable conversation history. For more information, see the following topics: [Managing the Archiving of internal and external communications in Skype for Business Server](#), [New-CsClientPolicy](#), and [Set-CsClientPolicy](#).

In order to archive transcripts to Exchange Server you must begin by configuring server-to-server authentication between Skype for Business Server and Exchange Server. After server-to-server authentication is in place, you can then carry out the following tasks in Skype for Business Server (note that, depending on your setup and configuration, you might not need to complete all of these tasks):

1. Enable Exchange archiving by modifying your Skype for Business Server archiving configuration settings. This step is required for all deployments.
2. Enable archiving for internal and/or external communications for your users. This step is required for all deployments.
3. Configure the ExchangeArchivingPolicy property for each user. This step is only required if Skype for Business Server and Exchange Server are located in different forests.

## Step 1: Enabling Exchange Archiving

Archiving in Skype for Business Server is primarily managed by using the archiving configuration settings. When you install Skype for Business Server you are automatically given a single, global collection of these settings. (Administrators can optionally create new collections of archiving settings at the site scope.) By default, archiving is not enabled in the global settings, nor is Exchange archiving enabled in these settings. In order to use Exchange archiving, administrators must configure both the EnableArchiving and the EnableExchangeArchiving properties in these configuration settings. The EnableArchiving property can be set to one of three possible values:

- **None.** Archiving is disabled. This is the default value. If EnableArchiving is set to None then nothing will be archived in either your Skype for Business Server archiving database or in Exchange Server.
- **ImOnly.** Only instant message transcripts are archived. If Exchange archiving is enabled, these transcripts will be archived in Exchange Server. If Exchange archiving is disabled then these transcripts will be archived



to Skype for Business Server.

- **ImAndWebConf.** Both instant message transcripts and Web conferencing transcripts are archived. If Exchange archiving is enabled these transcripts will be archived in Exchange Server. If Exchange archiving is disabled then these transcripts will be archived to Skype for Business Server.

The EnableExchangeArchiving property is a Boolean value: set EnableExchangeArchiving to True (\$True) to enable Exchange archiving or set EnableExchangeArchiving to False (\$False) to disable Exchange archiving. For example, this command enables the archiving of instant messaging transcripts and also enables Exchange archiving:

```
Set-CsArchivingConfiguration -Identity "global" -EnableArchiving ImOnly -EnableExchangeArchiving $True
```

To disable Exchange archiving, use a command similar to the following, which enables instant messaging archiving but disables archiving to Exchange (in other words, transcripts will be archived to Skype for Business Server):

```
Set-CsArchivingConfiguration -Identity "global" -EnableArchiving ImOnly -EnableExchangeArchiving $False
```

#### NOTE

If the EnableArchiving property is set to None, then Skype for Business Server will not archive instant messaging and Web conferencing transcripts at all. In that case, the server will simply ignore the value configured for EnableExchangeArchiving.

Exchange archiving can also be enabled (or disabled) by using the Skype for Business Server. To do that, complete the following procedure:

1. In Control Panel, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
2. On the **Archiving Configuration** tab, double-click the collection of archiving settings to be modified (for example, the **Global** collection).
3. In the **Edit Archiving Setting** pane, click the **Archiving setting** dropdown list and select either **Archive IM sessions** (to archive just instant messaging sessions) or **Archive IM and web conferencing sessions** (to archive both instant messaging and Web conferencing sessions).
4. After choosing the items to be archived, select the **Exchange Server integration** checkbox to enable Exchange archiving. To disable Exchange archiving, clear this checkbox.

#### NOTE

The **Exchange Server integration** checkbox will not be available if the **Archiving setting** is set to **Disable archiving**. You must enable archiving first and then enable Exchange archiving.

If Skype for Business Server and Exchange Server are located in the same forest, then archiving for individual users (or at least for users who have email accounts on Exchange Server) is managed by using Exchange In-Place Hold policies. If you have users who are homed on a previous version of Exchange then archiving for those users will be managed by using Skype for Business Server archiving policies. Note that only users with accounts on Exchange Server 2016 or Exchange Server 2013 can have their Skype for Business transcripts archived to Exchange.

If Skype for Business Server and Exchange Server are located in different forests then archiving for individual users is managed by configuring the ExchangeArchivingPolicy property for each individual user account. See Step 3 for more information.

## Step 2: Enabling the Archiving of Internal and/or External Communications

After you have enabled archiving (and Exchange archiving) you must then modify the appropriate archiving policies to ensure that user sessions are actually archived. Note that simply enabling archiving (Step 1) does not cause Skype for Business Server to begin archiving instant messaging and Web conferencing transcripts. Instead, you must use archiving policies to enable internal and/or external archiving. When you install Skype for Business Server you also install a single, global archiving policy that contains two properties:

- **ArchiveInternal.** When set to True (\$True) indicates that internal communication sessions involving only users who have Active Directory accounts in your organization) will be archived.
- **ArchiveExternal.** When set to True (\$True) indicates that internal communication sessions (sessions involving at least one user who does not have an Active Directory account in your organization) will be archived.

By default, both of these property values are set to False, meaning that neither internal nor external communication sessions are archived. To modify the global policy, you can use the Skype for Business Server Management Shell and the Set-CsArchivingPolicy cmdlet. This command enables the archiving of both internal and external communication sessions:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True -ArchiveExternal $True
```

Alternatively, you can use the New-CsArchivingPolicy to create a new policy at either the site scope or the per-user scope. For example, this command creates a new per-user archiving policy named RedmondArchivingPolicy:

```
New-CsArchivingPolicy -Identity "RedmondArchivingPolicy" -ArchiveInternal $True -ArchiveExternal $True
```

If you create a per-user policy you will then need to assign that policy to the appropriate users. For example:

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName "RedmondArchivingPolicy"
```

Archiving policies can also be managed by using the Skype for Business Server Control Panel. Within the Control Panel, click **Monitoring and Archiving** and then click **Archiving Policy**. To modify an existing policy, double-click the policy (e.g., Global) and then, in the **Edit Archiving Policy** pane, select or clear the **Archive internal communications** and the **Archive external communications** checkboxes as needed. To create a new archiving policy, click **New** and then select either **Site policy** or **User policy**. If you create a new user policy then you must access the appropriate user accounts (from the **Users** tab) and assign those users the new policy.

## Step 3: Configuring the ExchangeArchivingPolicy Property

If Skype for Business Server and Exchange Server are located in different forests, then it is not enough to simply enable Exchange archiving in the archiving configuration settings; that will not result in instant messaging and Web conferencing transcripts being archived in Exchange. Instead, you must also configure the ExchangeArchivingPolicy property on each of the relevant Skype for Business Server user accounts. This property can be set to one of four possible values:

1. **Uninitialized.** Indicates that archiving will be based on the In-Place Hold settings configured for the user's Exchange mailbox; if In-Place Hold has not been enabled on the user's mailbox then the user will have his or her messaging and Web conferencing transcripts archived in Skype for Business Server.
2. **UseLyncArchivingPolicy.** Indicates that the user's instant messaging and Web conferencing transcripts should be archived in Skype for Business Server rather than in Exchange.

3. **NoArchiving**. Indicates that the user's instant messaging and Web conferencing transcripts should not be archived at all. Note that this setting overrides any Skype for Business Server archiving policies assigned to the user.
4. **ArchivingToExchange**. Indicates that the user's instant messaging and Web conferencing transcripts should be archived to Exchange regardless of the In-Place Hold settings that have (or have not) been assigned to the user's mailbox.

For example, to configure a user account so that instant messaging and Web conferencing transcripts are always archived to Exchange you can use a command similar to this from the Skype for Business Server Management Shell:

```
Set-CsUser -Identity "Ken Myer" -ExchangeArchivingPolicy ArchivingToExchange
```

If you want to set the same archiving policy for a group of users (for example, all the users homed on a specified Registrar pool) you can use a command similar to this:

```
Get-CsUser -Filter {RegistrarPool -eq "atl-cs-001.litwareinc.com"} | Set-CsUser -ExchangeArchivingPolicy ArchivingToExchange
```

Note that you must use the Skype for Business Server Management Shell (and Windows PowerShell) in order to configure value of the ExchangeArchivingPolicy property. This property is not exposed to administrators in the Skype for Business Server.

If you would like to view a list of all the users who have been assigned a specific archiving policy then you can use a command similar to the following, which returns the Active Directory display name of all the users who have had the ExchangeArchivingPolicy property set to Uninitialized:

```
Get-CsUser | Where-Object {$_.ExchangeArchivingPolicy -eq "Uninitialized"} | Select-Object DisplayName
```

Likewise, this command returns the display name of the users who have not have the ExchangeArchivingPolicy property set to UseLyncArchivingPolicy:

```
Get-CsUser | Where-Object {$_.ExchangeArchivingPolicy -ne "UseLyncArchivingPolicy"} | Select-Object DisplayName
```

# Configure SharePoint Server to search for archived Skype for Business data

8/7/2019 • 4 minutes to read

**Summary:** Configure SharePoint Server to search for data archived by Exchange Server 2016 or Exchange Server 2013 and Skype for Business Server.

One of the major advantages to storing instant messaging and Web conferencing transcripts in Exchange Server instead of Skype for Business Server is that storing data in the same location allows administrators to use a single tool to search for archived Exchange data and/or archived Skype for Business Server data. Because all the data is stored in the same place (Exchange) any tool that can search for archived Exchange data can also search for archived Skype for Business Server data.

One tool that makes it easy to search for archived data is Microsoft SharePoint Server 2013. If you would like to use SharePoint to search for Skype for Business Server data, you must first complete all the steps involved in configuring Exchange archiving in Skype for Business Server. After Exchange Server and Skype for Business Server have been successfully integrated, you must then install the Exchange [Web Services Managed API](#) on your SharePoint Server. The downloaded file (EWSManagedAPI.msi) can be saved to any folder on your SharePoint server.

After the file has been downloaded complete the following procedure on the SharePoint server:

1. Open a command window by clicking **Start**, clicking **All Programs**, clicking **Accessories**, right-clicking **Command Prompt**, and then clicking **Run as administrator**.
2. In the command window, use the cd command to change the current directory to the folder where the file EWSManagedAPI.msi has been saved. For example, if you have saved the file to C:\Downloads type the following command in the command window and then press Enter:

```
cd C:\Downloads
```

3. To install the API, type the following command then press Enter:

```
msiexec /I EwsManagedApi.msi addlocal="ExchangeWebServicesApi_Feature,ExchangeWebServicesApi_Gac"
```

4. After the API has been installed, reset IIS by typing the following command and pressing Enter:

```
iisreset
```

After Exchange Web Services has been installed you must then configure server-to-server authentication between SharePoint Server and Exchange Server. To do this, first open the SharePoint Management Shell and run the following set of commands:

```
New-SPTrustedSecurityTokenIssuer -Name "Exchange" -MetadataEndPoint
"https://autodiscover.litwareinc.com/autodiscover/metadata/json/1"
$service = Get-SPSecurityTokenServiceConfig
$service.HybridStsSelectionEnabled = $True
$service.AllowMetadataOverHttp = $False
$service.AllowOAuthOverHttp = $False
$service.Update()
```

#### NOTE

Be sure and use the URI for your autodiscover service. Do not use the sample URI <https://autodiscover.litwareinc.com/autodiscover/metadata/json/1>.

After you have created the token issuer and configured the token service, run these commands, making sure to substitute the URL of your SharePoint site for the sample URL <http://atl-sharepoint-001>:

```
$exchange = Get-SPTrustedSecurityTokenIssuer "Exchange"
$app = Get-SPAppPrincipal -Site "https://atl-sharepoint-001" -NameIdentifier $exchange.NameID
$site = Get-SPSite "https://atl-sharepoint-001"
Set-SPAppPrincipalPermission -AppPrincipal $app -Site $site.RootWeb -Scope "SiteSubscription" -Right
"FullControl" -EnableAppOnlyPolicy
```

To configure server-to-server authentication for Exchange Server, open the Exchange Management Shell and run a command similar to this (assuming that Exchange has been installed on drive C: and that it uses the default folder path):

```
"C:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartnerApplication.ps1 -
AuthMetadataUrl 'https://atl-sharepoint-001/_layouts/15/metadata/json/1' -ApplicationType SharePoint"
```

After configuring the partner application it is recommended that you stop and restart Internet Information Services (IIS) on all your Exchange mailbox and client access servers. You can restart IIS by using a command similar to this, which restarts the service on the computer atl-exchange-001:

```
iisreset atl-exchange-001
```

This command can be run from within the Exchange Management Shell or from any other command window.

Next, run a command similar to the following, which gives the specified user (in this example, kenmyer) the right to do discovery on Exchange:

```
Add-RoleGroupMember "Discovery Management" -Member "kenmyer"
```

After server-to-server authentication has been established between Exchange and SharePoint, your next step is to create an eDiscovery site in SharePoint. That can be done by running commands similar to these from the SharePoint Management Shell:

```
$template = Get-SPWebTemplate | Where-Object {$_.Title -eq "eDiscovery Center"}
New-SPSite -Url "https://atl-sharepoint-001/sites/discovery" -OwnerAlias "kenmyer" -Template $Template -Name
"Discovery Center"
```

#### NOTE

"eDiscovery" is short for "electronic discovery," and typically refers to the process of looking through electronic archives for items that can be "reasonably calculated to lead to admissible evidence" in a court of law.

When the new site is ready, the next step is to configure Exchange Server to act as a result source for SharePoint. You can do that by completing the following procedure from the SharePoint Central Administration page:

1. On the Central Administration page click **Manage Service Applications** and then click **Search Service Application**.
2. On the Search Service Application: Search Administration page click **Result Sources** and then click **New Result Source**.
3. In the **New Result Source** pane enter a name for the new result source (for example, **Microsoft Exchange**) in the **Name** box. Select **Exchange** as the result source **Protocol**, and then enter the web services source URL for your Exchange server in the **Exchange Source URL** box. The source URL should look similar to this:

<https://atl-exchange-001.litwareinc.com/ews/exchange.asmx>

4. Make sure that **Use Autodiscover** is not selected, and then click **OK**.

Finally, create a new eDiscovery case and a new eDiscovery set by completing the following procedure from the SharePoint Discovery site (for example, <https://atl-sharepoint-001/sites/discovery>):

1. On the Site Contents page click **Create a new case**.
2. On the Site Contents: New SharePoint Site page, enter the user's email alias (for example, **kenmyer**) in the **Title** box, then add that same URL to the **Web Site Address** box. That will result in a URL similar to this:  
<https://atl-sharepoint-001/sites/eDiscovery/kenmyer>
3. Click **Create**.
4. When the eDiscovery set page appears, click **new item** under **Identity and Preserve: Discovery Sets**.
5. On the New: Discovery Set page, enter the user's email alias in the **Discovery Set Name** box. Enter **eDiscovery Lync\\*** in the **Filter** box and then click **Add & Manage Sources**.
6. On the Add & Manage Sources page, enter the user's email alias in the first textbox under **Mailboxes**. Click the check mailbox icon located next to the textbook to verify that SharePoint can connect to the specified mailbox.
7. Click **OK**.
8. On the eDiscovery set page, click **Save** to save the new eDiscovery set.

At this point you can search the specified mailbox (kenmyer) and/or enable In-Place holds the same way you would for any other SharePoint content or result source.

# Configure the use of high-resolution photos in Skype for Business Server

10/9/2019 • 3 minutes to read

**Summary:** Configure the use of high-resolution photos in Exchange Server 2019, Exchange Server 2016, Exchange Server 2013, or Exchange Online and Skype for Business Server.

In Skype for Business Server, photos can be stored in a user's Exchange Server 2019, Exchange Server 2016, Exchange Server 2013, or Exchange Online mailbox, which allows for photo sizes up to 648 pixels by 648 pixels. In addition, Exchange Server can automatically resize these photos for use in different products as needed. Typically that means three different photo sizes and resolutions:

- 64 pixels by 64 pixels, the size used for the Active Directory thumbnailPhoto attribute. If you upload a photo to Exchange Server, Exchange will automatically create a 64 pixel by 64 pixel version of that photo and update the user's thumbnailPhoto attribute. Note, however, that the reverse is not true: if you manually update the thumbnailPhoto attribute in Active Directory the photo in the user's Exchange mailbox will not automatically be updated.
- 96 pixels by 96 pixels, for use in Microsoft Outlook 2013 Web App, Microsoft Outlook 2013, Skype for Business Web App, and Skype for Business.
- 648 pixels by 648 pixels for use in Skype for Business and Skype for Business Web App Skype for Business Web App.

## NOTE

If you have the resources, it is recommended that you upload 648 x 648 photos; that provides the maximum resolution and optimal picture quality in any of the Office 2013 applications. Each JPEG photo with a size of 648 x 648 and a depth of 24 bits results in a file size of approximately 240 kilobytes. That means you will need approximately 1 megabyte of disk space for every 4 user photos.

High-resolution photos, which are accessed by using Exchange Web Services, can be uploaded by users who are running Outlook 2013 Web App; users are only allowed to update their own photo. Administrators, however, can update the photo for any user by using the Exchange Management Shell and a series of Windows PowerShell commands similar to the following:

```
$photo = ([Byte[]] $(Get-Content -Path "C:\Photos\Kenmyer.jpg" -Encoding Byte -ReadCount 0))
Set-UserPhoto -Identity "Ken Myer" -PictureData $photo -Preview -Confirm:$False
Set-UserPhoto -Identity "Ken Myer" -Save -Confirm:$False
```

The first command in the preceding example uses the `Get-Content` cmdlet to read the contents of the file `C:\Photos\Kenmyer.jpg` and store that data in a variable named `$photo`. In the second command, the Exchange cmdlet `Set-UserPhoto` is used to upload the photo and attach that photo to Ken Myer's user account.

## NOTE

In this example, Ken Myer's Active Directory display name is used as the user account Identity. You can also reference a user account by using other identifiers such as the user's SMTP address or his or her User Principal Name. See the documentation for the `Set-UserPhoto` cmdlet at <https://go.microsoft.com/fwlink/p/?LinkId=268536> for more information

Uploading the photo does not equate to assigning that photo to Ken Myer's user account. Instead, uploading the photo simply results in a preview of that photo to be displayed on the Outlook Web App Options page. To actually assign that photo to the user account the user must click **Save** on the Options page or the administrator must execute the third command in the example. That third command uses the Save parameter to assign the photo to Ken Myer's user account:

```
Set-UserPhoto -Identity "Ken Myer" -Save -Confirm:$False
```

To verify that the new photo has been assigned to the user account, Ken Myer can log on to Skype for Business, select **Options**, and then select **My Picture**. The newly-uploaded photo should be displayed as Ken's personal photo. Alternatively, administrators can verify the photo for any user by starting Internet Explorer and navigating to a URL similar to this:

```
https://atl-mail-001.litwareinc.com/ews/Exchange.asmx/s/GetUserPhoto?  
email=kenmyer@litwareinc.com&size=HR648x648
```

If the administrator can view the photo using Internet Explorer but the user cannot view his or her photo in Skype for Business there may be a connectivity problem with Exchange Web Services or with the Exchange autodiscover service.

Note, too that no additional configuration is required in order to make this photo available in Skype for Business. Instead, the photo will be instantly available after it has been uploaded and the `Set-UserPhoto` cmdlet has been run.



# Configure Skype for Business Server to use the unified contact store

8/7/2019 • 7 minutes to read

**Summary:** Configure the unified contacts store for Exchange Server 2016 or Exchange Server 2013 and Skype for Business Server.

Using the unified contact store, users maintain a single contacts list and then have those contacts available in multiple applications, including Skype for Business, Microsoft Outlook 2013, and Microsoft Outlook Web App 2013. When you enable the unified contact store for a user, that user's contacts are not stored in Skype for Business Server and retrieved as needed. Instead, his or her contacts are stored in Exchange Server 2016 or Exchange Server 2013 and are retrieved by using Exchange Web Services.

## NOTE

Technically, contact information is stored in a pair of folders found in the user's Exchange mailbox. The contacts themselves are stored in a folder named Skype for Business Contacts which is visible to end users; metadata about the contacts are stored in a subfolder that is not visible to end users.

## Enabling the Unified Contact Store for a User

If server-to-server authentication between Skype for Business Server and Exchange Server is already configured, then you have also enabled the unified contact store; no additional server configuration is required. However, additional user account configuration is required in order to move a user's contacts into the unified contact store. By default, user contacts are kept in Skype for Business Server and not in the unified contact store.

Access to the unified contact store is managed by using Skype for Business Server user services policies. User server policies have only a single property (UcsAllowed); this property is used to determine the location where a user's contacts are stored. If a user is managed by a user services policy where UcsAllowed has been set to True (\$True) then the user's contacts will be stored in the unified contact store. If the user is managed by a user services policy where UcsAllowed has been set to False (\$False) then his or her contacts will be stored in Skype for Business Server.

When you install Skype for Business Server, a single user services policy (configured at the global scope) is installed as well. The UcsAllowed value in this policy is set to True, meaning that, by default, user contacts will be stored in the unified contact store (assuming this has been deployed and configured). If you want to migrate all of your user contacts to the unified contact store you do not have to do anything at all.

If you would prefer not to migrate all your contacts to the unified contact store you can disable the unified contact store for all users by setting the UcsAllowed property in the global policy to False:

```
Set-CsUserServicesPolicy -Identity global -UcsAllowed $False
```

After you have disabled the unified contact store in the global policy you can then create a per-user policy that enables the use of the unified contact store; this allows you to have some users keep their contacts in the unified contact store while other users continue to keep their contacts in Skype for Business Server. You can create a per-user user services policy by using a command similar to this:

```
New-CsUserServicesPolicy -Identity "AllowUnifiedContactStore" -UcsAllowed $True
```

After you have created the new policy you must then assign that policy to any user who should have access to the unified contact store. Per-user policies can be assigned to users by using commands similar to this:

```
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName "AllowUnifiedContactStore"
```

After the policy has been assigned, Skype for Business Server will begin to migrate the user's contacts to the unified contact store. After migration is complete, the user will then have his or her contacts stored in Exchange rather than Skype for Business Server. If the user happens to be logged on to Lync 2013 at the time migration completes, a message box will appear and he or she will be asked to log off of Skype for Business and then log back on in order to finalize the process. Users who have not been assigned this per-user policy will not have their contacts migrated to the unified contact store. That's because those users are being managed by the global policy, and use of the unified contact store has been disabled in the global policy.

You can verify that a user's contacts have successfully been migrated to the unified contact store by running the [Test-CsUnifiedContactStore](#) cmdlet from within the Skype for Business Server Management Shell:

```
Test-CsUnifiedContactStore -UserSipAddress "sip:kenmyer@litwareinc.com" -TargetFqdn "atl-cs-001.litwareinc.com"
```

If `Test-CsUnifiedContactStore` succeeds that means that the contacts for the user `sip:kenmyer@litwareinc.com` have been migrated to the unified contact store.

## Rolling Back the Unified Contact Store

If you need to remove a user's contacts from the unified contact store (for example, if the user needs to be rehomed on Microsoft Lync Server 2010 and thus can no longer use the unified contact store) you must do two things. First, you must assign the user a new user services policy, one that prohibits storing contacts in the unified contact store. (That is, a policy where the `UcsAllowed` property has been set to `$False`.) If you do not have such a policy you can create one using a command similar to this:

```
New-CsUserServicesPolicy -Identity NoUnifiedContactStore -UcsAllowed $False
```

You can then assign this new per-user policy (`NoUnifiedContactStore`) by using a command like this:

```
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName NoUnifiedContactStore
```

The preceding command assigns the new policy to the user Ken Myer, and also prevents Ken's contacts from being migrated to the unified contact store.

### NOTE

In some cases you can achieve the same net effect by simply un-assigning the user's current user services policy. For example, suppose Ken Myer has a per-user user services policy that enables the unified contact store, but your global policy prohibits the use of the unified contact store. In that case, you could un-assign Ken's per-user services policy. When you do that, Ken will automatically be managed by the global policy, and thus will no longer have access to the unified contact store. To un-assign a previously-assigned per-user policy, use the same command as shown before, but this time set the `PolicyName` parameter to a null value: `Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName $Null`

The terminology "prevents Ken's contacts from being migrated to the unified contact store" is important to keep in

mind when working with the unified contact store. Simply assigning Ken a new user services policy will not move his contacts out of the unified contact store. When a user logs on to Skype for Business Server, the system checks the user's user services policy to see whether his or her contacts should be kept in the unified contact store. If the answer is yes (that is, if the `UcsAllowed` property is set to `$True`) then those contacts will be migrated to the unified contact store (assuming that those contacts are not already in the unified contact store). If the answer is no, then Skype for Business Server simply ignores the user's contacts and moves on to its next task. That means that Skype for Business Server will not automatically move a user's contacts from out of the unified contact store, regardless of the value of the `UcsAllowed` property.

That also means that, after assigning the user a new user services policy, you must then run the [Invoke-CsUcsRollback](#) cmdlet in order to move the user's contacts out of Exchange Server and back to Skype for Business Server. For example, after assigning Ken Myer a new user services policy you can then move his contacts out of the unified contact store by using the following command:

```
Invoke-CsUcsRollback -Identity "Ken Myer"
```

If you change the user services policy but do not run the `Invoke-CsUcsRollback` cmdlet Ken's contacts will not be removed from the unified contact store. What if you run `Invoke-CsUcsRollback` but do not change Ken Myer's user services policy? In that case, Ken's contacts will be temporarily removed from the unified contact store. The fact that this removal is temporary is important to keep in mind. After Ken's contacts have been removed from the unified contact store, Skype for Business Server will wait 7 days and then check to see which user services policy has been assigned to Ken. If Ken is still assigned a policy that enables the user of the unified contact store, then his contacts will automatically be moved back to into the contact store. To permanently remove contacts from the unified contact store you must change the user services policy in addition to running the `Invoke-CsUcsRollback` cmdlet.

Due to the large number of variables that can affect migration, it is difficult to estimate how long it will take before accounts are fully migrated to the unified contact store. As a general rule, however, migration does not take effect immediately: even when migrating a small number of contacts it might take 10 minutes or more before the move is complete.

# Configure Exchange Server Unified Messaging for Skype for Business Server voice mail

8/7/2019 • 11 minutes to read

**Summary:** Configure Exchange Server Unified Messaging for Skype for Business Server voice mail.

Skype for Business Server enables you to have voicemail messages stored in Exchange Server 2016 or Exchange Server 2013; those voicemail messages will then appear as email messages in your users' Inboxes.

## NOTE

Exchange Unified Messaging as previously known is no longer available in Exchange 2019, but you can still use Phone System to record voicemail messages and then leave the recording in a user's Exchange mailbox. See [Plan Cloud Voicemail service](#) for more information.

If you have already configured server-to-server authentication between Skype for Business Server and Exchange Server 2016 or Exchange Server 2013, then you are ready to setup unified messaging. To do so, you must first create and assign a new unified messaging dial plan on your Exchange Server. For example, these two commands (run from within the Exchange Management Shell) configure a new 3-digit dial plan for Exchange:

```
New-UMDialPlan -Name "RedmondDialPlan" -VoIPSecurity "Secured" -NumberOfDigitsInExtension 3 -URIType "SipName" -CountryOrRegionCode 1
Set-UMDialPlan "RedmondDialPlan" -ConfiguredInCountryOrRegionGroups "Anywhere,*,*,*" - AllowedInCountryOrRegionGroups "Anywhere"
```

In the first command in the example, the VoIPSecurity parameter, and the parameter value "Secured" indicates that the signaling channel is encrypted by using Transport Layer Security (TLS). The URIType "SipName" indicates that messages will be sent and received using the SIP protocol, and the CountryOrRegionCode of 1 indicates that the dial plan applies to the US.

In the second command, the parameter value passed to the ConfiguredInCountryOrRegionGroups parameter specifies the in-country groups that can be used with this dial plan. The parameter value "Anywhere,\*,\*,\*" sets the following:

- Group name ("Anywhere")
- AllowedNumberString (\*, a wildcard character indicating that any number string is allowed)
- DialNumberString (\*, a wildcard character indicating that any dialed number is allowed)
- TextComment (\*, a wildcard character indicating that any text command is allowed)

## NOTE

Creating a new dial plan will also create a Default Mailbox Policy.

After creating and configuring the new dial plan you must add the new dial plan to your unified messaging server and then modify the startup mode of that server; in particular, you must set the startup mode to "Dual". You can perform both of these tasks from within the Exchange Management Shell:

```
Set-UmService -Identity "atl-exchangeum-001.litwareinc.com" -DialPlans "RedmondDialPlan" -UMStartupMode "Dual"
```

After the unified messaging server has been configured you should next run the `Enable-ExchangeCertificate` cmdlet to ensure that your Exchange certificate is applied to the unified messaging service:

```
Enable-ExchangeCertificate -Server "atl-umserver-001.litwareinc.com" -Thumbprint  
"EA5A332496CC05DA69B75B66111C0F78A110D22d" -Services "SMTP","IIS","UM"
```

After the certificate has been correctly assigned you must then stop and restart the `MsExchangeUM` service on the unified messaging server. This service must be stopped and restarted any time you change the startup mode.

After finishing configuration of the unified messaging server you can then configure the UM Call Router:

```
Set-UMCallRouterSettings -Server "atl-exchange-001.litwareinc.com" -UMStartupMode "Dual" -DialPlans  
"RedmondDialPlan"  
Enable-ExchangeCertificate -Server "atl-umserver-001.litwareinc.com" -Thumbprint  
"45BAA32496CC891169B75B9811320F78A1075DDA" -Services "IIS","UMCallRouter"
```

Because the startup mode has changed you must stop and restart the `MsExchangeUMCR` service on the computer hosting the UM Call Router.

To complete the unified messaging setup, you then need to create a UM mailbox policy and then use that policy to enable users for unified messaging. You can create a mailbox policy by using a command similar to this:

```
New-UMMailboxPolicy -Name "RedmondMailboxPolicy" -AllowedInCountryOrRegionGroups "Anywhere"
```

And you can enable a user for unified messaging by using a command similar to this:

```
Enable-UMMailbox -Extensions 100 -SIPResourceIdentifier "kenmyer@litwareinc.com" -Identity  
"litwareinc\kenmyer" -UMMailboxPolicy "RedmondMailboxPolicy"
```

In the preceding command, the `Extensions` parameter represents the telephone extension number for the user. In this example, the user has the extension number 100.

After you have enabled his mailbox, the user `kenmyer@litwareinc.com` should be able to use Exchange unified messaging. You can verify that the user can connect to Exchange UM by running the [Test-CsExUMConnectivity](#) cmdlet from within the Skype for Business Server Management Shell:

```
$credential = Get-Credential "litwareinc\kenmyer"  
Test-CsExUMConnectivity -TargetFqdn "atl-cs-001.litwareinc.com" -UserSipAddress "sip:kenmyer@litwareinc.com" -  
UserCredential $credential
```

If you have a second user who has been enabled for unified messaging you can use the [Test-CsExUMVoiceMail](#) cmdlet to verify that this second user can leave a voicemail message for the first user.

```
$credential = Get-Credential "litwareinc\pilar"  
Test-CsExUMVoiceMail -TargetFqdn "atl-cs-001.litwareinc.com" -ReceiverSipAddress "sip:kenmyer@litwareinc.com" -  
-SenderSipAddress "sip:pilar@litwareinc.com" -SenderCredential $credential
```

## Configuring Unified Messaging on Microsoft Exchange Server

## IMPORTANT

If you want to use Exchange Unified Messaging (UM) to provide call answering, Outlook Voice Access, or auto-attendant services for Enterprise Voice users, read [Plan for Exchange Unified Messaging integration in Skype for Business](#), and then follow the instructions in this section.

To configure Exchange Unified Messaging (UM) to work with Enterprise Voice, you'll need to perform the following tasks:

- Configure certificates on the server running Exchange Unified Messaging (UM) services

### NOTE

Add all Client Access and Mailbox servers to all UM SIP URI dial plans. If not, outbound call routing won't work as expected.

- Create one or more UM SIP URI dial plans, along with the subscriber access phone numbers, as needed, and then create corresponding L dial plans.
- Use the `exchucutil.ps1` script to:
  - Create UM IP gateways.
  - Create UM hunt groups.
  - Grant Skype for Business Server permission to read UM Active Directory Domain Services objects.
- Create a UM auto-attendant object.
- Create a subscriber access object.
- Create a SIP URI for each user and associating users with a UM SIP URI dial plan.

## Requirements and Recommendations

Before you begin, the documentation in this section assumes that you have deployed the following Exchange roles: Client Access and Mailbox. In Microsoft Exchange Server, Exchange UM runs as a service on these servers.

Also note the following:

- If Exchange UM is installed in multiple forests, the Exchange Server integration steps must be performed for each UM forest. In addition, each UM forest must be configured to trust the forest in which Skype for Business Server is deployed, and the forest in which Skype for Business Server is deployed must be configured to trust each UM forest.
- Integration steps are performed on both the Exchange Server roles where Unified Messaging services are running, and on the server running Skype for Business Server. You should perform the Exchange Server Unified Messaging integration steps before you perform the Lync Server 2013 integration steps.

### NOTE

To see which integration steps are performed on which servers and by which administrator roles, see [Deployment process overview for integrating on-premises Unified Messaging and Skype for Business](#).

The following tools must be available on each server running Exchange UM:

- Exchange Management Shell
- The script `exchucutil.ps1`, which performs the following tasks:
  - Creates a UM IP gateway for each Skype for Business Server.

- Creates a hunt group for each gateway. The pilot identifier of each hunt group specifies the UM SIP URI dial plan used by the Front End pool or Standard Edition server that is associated with the gateway.
- Grants Skype for Business Server permission to read Exchange UM objects in Active Directory Domain Services.

### Configure Unified Messaging on Microsoft Exchange with ExchUCUtil.ps1

When you're integrating Microsoft Skype for Business Server with Exchange Unified Messaging (UM), you have to run the ExchUcUtil.ps1 script in the Shell. The ExchUcUtil.ps1 script does the following:

- Creates a UM IP gateway for each Skype for Business Server pool.

#### IMPORTANT

The ExchUcUtil.ps1 script creates one or more UM IP gateways. You must disable outgoing calls on all UM IP gateways except one gateway that the script created. This includes disabling outgoing calls on UM IP gateways that were created before you ran the script.

- Creates a UM hunt group for each UM IP gateway. The pilot identifier of each hunt group specifies the UM SIP URI dial plan used by the Skype for Business Server Front End pool or Standard Edition server that's associated with the UM IP gateway.
- Grants Skype for Business Server permission to read Active Directory UM container objects such as UM dial plans, auto attendants, UM IP gateways, and UM hunt groups.

#### IMPORTANT

Each UM forest must be configured to trust the forest in which Skype for Business Server is deployed, and the forest in which Skype for Business Server 2013 is deployed must be configured to trust each UM forest. If Exchange UM is installed in multiple forests, the Exchange Server integration steps must be performed for each UM forest or you'll have to specify the Skype for Business Server domain. For example, ExchUcUtil.ps1 -Forest:.

### Use the Shell to run the ExchUcUtil.ps1 script

Run the ExchUcUtil.ps1 script on any Exchange server in your organization that's in the same topology as Skype for Business Server. You can run the script from a Mailbox server using the Shell or you can run the script using Remote Windows PowerShell on a Client Access server. If you run the script on a Client Access server in your organization, the Client Access server will proxy the Remote Windows PowerShell session to a Mailbox server in the organization.

#### IMPORTANT

The ExchUcUtil.ps1 script creates one or more UM IP gateways. You must disable outgoing calls on all UM IP gateways except one gateway that the script created. This includes disabling outgoing calls on UM IP gateways that were created before you ran the script. To disable outgoing calls on a UM IP gateway, see [Disable outgoing calls on UM IP gateways](#).

#### IMPORTANT

You must have the permissions of the Exchange Organization Management role or be a member of the Exchange Organization Administrators security group to run the script.

1. Open the Exchange Management Shell.
2. At the C:\Windows\System32 prompt, type **cd <drive letter>:\Program Files\Microsoft\Exchange Server\V15\Scripts>.ExchUcUtil.ps1**, and then press Enter.

### How do you know this worked?

To verify that the ExchUcUtl.ps1 script completed successfully, do the following:

- Use the Get-UMIPGateway cmdlet or the EAC to view the new UM IP gateway or gateways that were created.
- Use the Get-UMHuntGroup cmdlet or the EAC to view the new UM hunt group or groups that were created.

### Configure certificates on the server running Exchange Server Unified Messaging

If you have deployed Exchange Unified Messaging (UM), as described in Planning for Exchange Unified Messaging integration in Skype for Business Server in the Planning documentation, and you want to provide Exchange UM features to Enterprise Voice users in your organization, you can use the following procedures to configure the certificate on the server running Exchange UM.

#### IMPORTANT

For internal certificates, both the servers running Skype for Business Server and the servers running Microsoft Exchange must have trusted root authority certificates that are mutually trusted. The certification authority (CA) can either be the same, or a different certification authority, as long as the servers have the certification authority's root certificate registered in their trusted root authority certificate store.

The Exchange Server must be configured with a server certificate in order to connect to Skype for Business Server:

1. Download the CA certificate for the Exchange Server.
2. Install the CA certificate for the Exchange Server.
3. Verify that the CA is in the list of trusted root CAs of the Exchange Server.
4. Create a certificate request for the Exchange Server and install the certificate.
5. Assign the certificate for the Exchange Server.

#### To download the CA certificate:

1. On the server running Exchange UM, click **Start**, click **Run**, type **http://<name of your Issuing CA Server>/certsrv**, and then click **OK**.
2. Under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**.
3. Under **Download a CA Certificate, Certificate Chain, or CRL**, select **Encoding Method to Base 64**, and then click **Download CA certificate**.

#### NOTE

You can also specify Distinguished Encoding Rules (DER) encoding at this step. If you select DER encoding, the file type in the next step of this procedure and in step 10 of **To Install the CA certificate** is .p7b rather than .cer.

4. In the **File Download** dialog box, click **Save**, and then save the file to the hard disk on the server. (The file will have either a .cer or a .p7b file extension, depending on the encoding that you selected in the previous step.)

#### To install the CA certificate:

1. On the server running Exchange UM, open Microsoft Management Console (MMC) by clicking **Start**, clicking **Run**, typing **mmc** in the Open box, and then clicking **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Add Standalone Snap-ins** box, click **Certificates**, and then click **Add**.
4. In the **Certificate snap-in** dialog box, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, verify that the **Local computer: (the computer this console is running on)** check box is selected, and then click **Finish**.
6. Click **Close**, and then click **OK**.



7. In the console tree, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
8. Right-click **Certificates**, click **All Tasks**, and click **Import**.
9. Click **Next**.
10. Click **Browse** to locate the file, and then click **Next**. (The file will have either a .cer or a .p7b file extension, depending on the encoding that you selected in step 3 of **To download the CA certificate**.)
11. Click **Place All Certificates** in the following store.
12. Click **Browse**, and then select **Trusted Root Certification Authorities**.
13. Click **Next** to verify the settings, and then click **Finish**.

**To verify that the CA is in the list of trusted root CAs:**

1. On the server running Exchange UM, in MMC expand Certificates (Local Computer), expand Trusted Root Certification Authorities, and then click Certificates.
2. In the details pane, verify that your CA is on the list of trusted CAs.

# Configure integration between on-premises Skype for Business Server and Outlook Web App

8/7/2019 • 3 minutes to read

**Summary:** Integrate Skype for Business Server and Outlook Web App.

Customers who are using on-premises Skype for Business Server deployments can configure interoperability with Microsoft Outlook Web App in Microsoft Exchange Online in a hybrid deployment mode. Interoperability features include single sign on and instant messaging (IM) and presence integration with the Outlook Web App interface. To enable this integration, you must configure the Edge Server in your on-premises Skype for Business Server deployment by completing the following tasks:

- Configure a shared SIP address space
- Configure a hosting provider on the Edge Server
- Verify replication of the updated Central Management store

## Configure a Shared SIP Address Space

To integrate on-premises Skype for Business Server with Exchange Online, you must configure a shared SIP address space. The same SIP domain address space is supported by both Skype for Business Server and the Exchange Online service.

Using the Skype for Business Server Management Shell, configure the Edge Server for federation by running the **Set-CsAccessEdgeConfiguration** cmdlet, using the parameters displayed in the following example:

```
Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
```

- **AllowFederatedUsers** parameter specifies whether internal users are allowed to communicate with users from federated domains. This property also determines whether internal users can communicate with users in a shared SIP address space scenario with Skype for Business Server and Exchange Online.

For details about using the Skype for Business Server Management Shell, see [Skype for Business Server Management Shell](#).

## Configure a Hosting Provider on the Edge Server

Using the Skype for Business Server Management Shell, configure a hosting provider on the Edge Server by running the **New-CsHostingProvider** cmdlet, using the parameters in the following example:

```
New-CsHostingProvider -Identity "Exchange Online" -Enabled $True -EnabledSharedAddressSpace $True -HostsOCSUsers $False -ProxyFqdn "exap.um.outlook.com" -IsLocal $False -VerificationLevel UseSourceVerification
```

#### NOTE

If you are using Office 365 operated by 21Vianet in China, replace the value for the ProxyFqdn parameter in this example ("exap.um.outlook.com") with the FQDN for the service operated by 21Vianet: "exap.um.partner.outlook.cn". If you are using Office 365 GCC High, replace the value for the ProxyFqdn parameter in this example ("exap.um.outlook.com") with the FQDN for GCC High: "exap.um.office365.us".

- **Identity** specifies a unique string value identifier for the hosting provider that you are creating (for example, "Exchange Online"). Values that contain spaces must be in double quotes.
- **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. This must be set to True.
- **EnabledSharedAddressSpace** indicates whether the hosting provider will be used in a shared SIP address space scenario. This must be set to True.
- **HostsOCSUsers** indicates whether the hosting provider is used to host Office Communications Server or Skype for Business Server. This must be set to False.
- **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider. For Exchange Online, the FQDN is exap.um.outlook.com.
- **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Skype for Business Server topology. This must be set to False.
- **VerificationLevel** Indicates the verification level allowed for messages that are sent to and from the hosted provider. Specify **UseSourceVerification**, which relies on the verification level included in messages sent from the hosting provider. If this level is not specified, the message will be rejected as being unverifiable.

## Verify Replication of the Updated Central Management Store

The changes you made by using the cmdlets in the preceding sections are automatically applied to the Edge Server, and generally take less than a minute to replicate. You can validate replication status, and then confirm that the changes were applied to your Edge Server by using the following cmdlets.

To verify replication updates, on a server internal in your Skype for Business Server deployment, run the following cmdlet:

```
Get-CsManagementStoreReplicationStatus
```

Check if UpToDate value is showing TRUE for all Replicas.

To confirm that the changes were applied, on the Edge Server, run the following cmdlet:

```
Get-CsHostingProvider -LocalStore
```

Double check if the information shown matches the changes committed in the previous steps.

## See also

[Providing Skype for Business Server users voice mail on hosted Exchange UM](#)

[Hosted Exchange Unified Messaging integration in Skype for Business Server](#)

# Configure Integration and OAuth between Skype for Business Online and Exchange Server

11/5/2019 • 5 minutes to read

Configuring integration between Exchange server and Skype for Business Online enables the Skype for Business and Exchange Integration features described in [Feature support](#).

This topic applies to integration with Exchange Server 2013 through 2019.

## What do you need to know before you begin?

- Estimated time to complete this task: 15 minutes
- You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the [Exchange and Shell infrastructure permissions](#) topic.
- For information about keyboard shortcuts that may apply to the procedures in this topic, see [Keyboard shortcuts in the Exchange admin center](#).
- For information about compatibility, see [Skype for Business compatibility with Office apps](#).

## Configure integration between Exchange Server and O365

### Step 1: Configure OAuth authentication between Exchange Server and O365

Perform the steps in the following article:

[Configure OAuth authentication between Exchange and Exchange Online organizations](#)

### Step 2: Create a new Mail User account for the Skype for Business Online Partner Application

This step is done on the Exchange server. It will create a mail user and assign it the appropriate management role rights. This account will then be used in the next step.

Specify a verified domain for your Exchange organization. This domain should be the same domain used as the primary SMTP domain used for the on-premises Exchange accounts. This domain is referred as <your Verified Domain> in the following procedure. Also, the <DomainControllerFQDN> should be the FQDN of a domain controller.

```
$user = New-MailUser -Name SfBOnline-ApplicationAccount -ExternalEmailAddress SfBOnline-ApplicationAccount@<your Verified Domain> -DomainController <DomainControllerFQDN>
```

This command will hide the new mail user from address lists.

```
Set-MailUser -Identity $user.Identity -HiddenFromAddressListsEnabled $True -DomainController <DomainControllerFQDN>
```

These next two commands will assign the UserApplication and ArchiveApplication management role to this new account.

```
New-ManagementRoleAssignment -Role UserApplication -User $user.Identity -DomainController <DomainControllerFQDN>
```

```
New-ManagementRoleAssignment -Role ArchiveApplication -User $user.Identity -DomainController
<DomainControllerFQDN>
```

### Step 3: Create and enable a Partner Application for Skype for Business Online

Create a new partner application and will use the account you just created. Run the following command in the Exchange PowerShell in your on-premises Exchange organization.

```
New-PartnerApplication -Name SfBOnline -ApplicationIdentifier 00000004-0000-0fff1-ce00-000000000000 -Enabled
$True -LinkedAccount $user.Identity
```

### Step 4: Export the on-premises authorization certificate

Run a PowerShell script to export the on-premises authorization certificate, which you will import to your Skype for Business Online organization in the next step.

Save the following text to a PowerShell script file named, for example, ExportAuthCert.ps1.

```
$thumbprint = (Get-AuthConfig).CurrentCertificateThumbprint
if((test-path $env:SYSTEMDRIVE\OAuthConfig) -eq $false)
{
md $env:SYSTEMDRIVE\OAuthConfig
}
cd $env:SYSTEMDRIVE\OAuthConfig
$oAuthCert = (dir Cert:\LocalMachine\My) | where {$_.Thumbprint -match $thumbprint}
$certType = [System.Security.Cryptography.X509Certificates.X509ContentType]::Cert
$certBytes = $oAuthCert.Export($certType)
$certFile = "$env:SYSTEMDRIVE\OAuthConfig\OAuthCert.cer"
[System.IO.File]::WriteAllBytes($certFile, $certBytes)
```

In Exchange PowerShell in your on-premises Exchange organization, run the PowerShell script that you just created. For example: .\ExportAuthCert.ps1

### Step 5: Upload the on-premises authorization certificate to Azure Active Directory ACS

Next, use Windows PowerShell to upload the on-premises authorization certificate that you exported in the previous step to Azure Active Directory Access Control Services (ACS). To do this, the Azure Active Directory Module for Windows PowerShell cmdlets must already be installed. If it's not installed, go to <https://aka.ms/aadposh> to install the Azure Active Directory Module for Windows PowerShell. Complete the following steps after the Azure Active Directory Module for Windows PowerShell is installed.

1. Click the **Azure Active Directory Module for Windows PowerShell** shortcut to open a Windows PowerShell workspace that has the Azure AD cmdlets installed. All commands in this step will be run using the Windows PowerShell for Azure Active Directory console.
2. Save the following text to a PowerShell script file named, for example, UploadAuthCert.ps1 .

```
Connect-MsolService;
Import-Module msonlineextended;
$CertFile = "$env:SYSTEMDRIVE\OAuthConfig\OAuthCert.cer"
$objFSO = New-Object -ComObject Scripting.FileSystemObject;
$CertFile = $objFSO.GetAbsolutePathName($CertFile);
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate
$cer.Import($CertFile);
$binCert = $cer.GetRawCertData();
$credValue = [System.Convert]::ToBase64String($binCert);
$ServiceName = "00000004-0000-0ff1-ce00-000000000000";
$p = Get-MsolServicePrincipal -ServicePrincipalName $ServiceName
New-MsolServicePrincipalCredential -AppPrincipalId $p.AppPrincipalId -Type asymmetric -Usage Verify -
Value $credValue
```

3. Run the PowerShell script that you created in the previous step. For example: `.\UploadAuthCert.ps1`
4. After you start the script, a credentials dialog box is displayed. Enter the credentials for the tenant administrator account of your Microsoft Online Azure AD organization. After running the script, leave the Windows PowerShell for Azure AD session open. You will use this to run a PowerShell script in the next step.

### Step 6: Verify that the Certificate has Uploaded to the Skype for Business Service Principal

1. In the PowerShell opened and authenticated to Azure Active Directory, run the following

```
Get-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000
```

2. Press Enter when prompted for ReturnKeyValues
3. Confirm you see a key listed with start date and end data that matches your Exchange OAuth certificate start and end dates

### Verify your success

Verify that the configuration is correct by verifying some of the features are working successfully.

1. Confirm that Skype for Business users with Cloud Voicemail service, in an organization with a Hybrid Exchange Server configuration, can successfully change their voicemail greetings.
2. Confirm conversation history for mobile clients is visible in the Outlook Conversation History folder.
3. Confirm that archived chat messages are deposited in the user's on-premises mailbox in the Purges folder using [EWSEditor](#).

Alternately, look at your traffic. The traffic in an OAuth handshake is really distinctive (and doesn't look like Basic authentication), particularly around realms, where you'll begin to see issuer traffic that looks like this: 00000004-0000-0ff1-ce00-000000000000@ (sometimes with a / before the @ sign), in the tokens that are being passed. You won't see a username or password, which is the point of OAuth. But you will see the 'Office' issuer – in this case '4' is Skype for Business – and the realm of your subscription.

If you want to be sure you're successfully using OAuth, make certain you know what to expect and know what the traffic should look like. So [here's what to expect](#), here's a pretty standard [example of OAuth traffic in a Microsoft application](#) (really helpful to read, though it doesn't use Refresh tokens), and there are Fiddler extensions that will let you look into your OAuth JWT (JSON Web Token).

Here's an [example of setting one up](#), but you can use any network tracing tool you like to undertake this process.

## Related topics

[Configure OAuth authentication between Exchange and Exchange Online organizations](#)



# Deploy unified contact store in Skype for Business Server

8/7/2019 • 5 minutes to read

**Summary:** Enable the unified contact store in Skype for Business Server.

Enabling unified contact store in Skype for Business Server does not require any topology settings. To enable unified contact store for users:

- Unified contact store policy is enabled (default is enabled).
- Users log in with Skype for Business at least once.

After a user's contacts have been migrated, which happens automatically when a user logs in with Skype for Business, the user can access and manage their Skype for Business contacts from Skype for Business, Outlook 2013, or Outlook Web Access. The user does not have to be logged in to Skype for Business to manage their contacts from Outlook or Outlook Web Access.

## IMPORTANT

If a user logs in from Skype for Business after migration, contacts and groups are available and up-to-date, but the user cannot manage (that is, add, delete, move, tag, untag, or modify) those contacts.

## Enable users for unified contact store

When you deploy Skype for Business Server and publish the topology, unified contact store is enabled for all users by default. You do not need to take any additional action to enable unified contact store after you deploy Skype for Business Server. However, you can use the **Set-CsUserServicesPolicy** cmdlet to customize which users have unified contact store available. You can enable this feature globally, by site, by tenant, or by individuals or groups of individuals.

### To enable users for unified contact store

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business**, and then click **Skype for Business Server Management Shell**.
2. Do any of the following:
  - To enable unified contact store globally for all Skype for Business Server users, enter the following cmdlet at the Windows PowerShell command-line interface:

```
Set-CsUserServicesPolicy -Identity global -UcsAllowed $True
```

- To enable unified contact store for the users at a specific site, at the prompt, type:

```
New-CsUserServicesPolicy -Identity site:<site name> -UcsAllowed $True
```

For example:

```
New-CsUserServicesPolicy -Identity site:Redmond -UcsAllowed $True
```



- To enable unified contact store by tenant, at the prompt, type:

```
Set-CsUserServicesPolicy -Tenant <tenantId> -UcsAllowed $True
```

For example:

```
Set-CsUserServicesPolicy -Tenant "38aad667-af54-4397-aaa7-e94c79ec2308" -UcsAllowed $True
```

- To enable unified contact store for specific users, at the prompt, type:

```
New-CsUserServicesPolicy -Identity "<policy name>" -UcsAllowed $True  
Grant-CsUserServicesPolicy -Identity "<user display name>" -PolicyName "<policy name>"
```

#### NOTE

You can also use user alias or SIP URI instead of the user display name.

For example:

```
New-CsUserServicesPolicy -Identity "UCS Enabled Users" -UcsAllowed $True  
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName "UCS Enabled Users"
```

#### NOTE

In the preceding example, the first command creates a new per-user policy named UCS Enabled Users with the UcsAllowed flag set to True. The second command assigns the policy to the user with the display name Ken Myer, which means that Ken Myer is now enabled for unified contact store.

## Migrate users to unified contact store

A user's contacts are automatically migrated to the Exchange 2013 server when the user:

- Has been assigned a user services policy that has UcsAllowed set to True.
- Has been provisioned with an Exchange 2013 mailbox and has signed into the mailbox at least once.
- Logs in by using a Skype for Business rich client.

If the user logs in with a Lync or earlier client, or if the user is not connected to an Exchange 2013 server, the user services policy is ignored and the user's contacts remain in Skype for Business Server.

You can determine whether a user's contacts have been migrated by using either of the following methods:

- Check the following registry key on the client computer:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\<SIP URL>\UCS
```

If the user's contacts are stored in Exchange 2013, this key contains a value of InUCSMode with a value of 2165.

- Run the **Test-CsUnifiedContactStore** cmdlet. At the Skype for Business Server Management Shell command line, type:

```
Test-CsUnifiedContactStore -UserSipAddress "sip:kenmyer@litwareinc.com" -TargetFqdn "at1-cs-001.litwareinc.com"
```

If **Test-CsUnifiedContactStore** succeeds, the user's contacts were migrated to unified contact store.

## Roll Back Migrated Users

If you need to roll back the unified contact store feature, roll back the contacts only if you move the user back to Exchange 2010 or Lync Server 2010. To roll back, disable the policy for the user, and then run the **Invoke-CsUcsRollback** cmdlet. Just running **Invoke-CsUcsRollback** alone is not enough to ensure permanent rollback, because unified contact store migration will be initiated again if the policy is not disabled. For example, if a user is rolled back because Exchange 2013 is rolled back to Exchange 2010, and then the user's mailbox is moved to Exchange 2013, the unified contact store migration will be initiated again seven days after the rollback, as long as unified contact store is still enabled for the user in the user services policy.

The **Move-CsUser** cmdlet automatically rolls back the user's contact store from Exchange 2013 to Skype for Business Server in the following situations:

- When users are moved from Skype for Business Server to Microsoft Lync Server 2013 or Lync Server 2010.
- When users are migrated cross premises, such as when a user is moved from Skype for Business Online to Skype for Business Server on-premises, or vice versa.

Importing unified contact store data from a backup database can cause unified contact store data and user data to become corrupted if the unified contact store mode changed between the export and the import. For example:

- If you export contact lists before the users' contacts are migrated to Exchange 2013 and then, after the migration, import the same data, the unified contact store data and contact lists will be corrupted.
- If you export user data after you migrate users to Exchange 2013, roll back the migration, and then for some reason you import the data from after the migration, the unified contact store data and contact lists will be corrupted.

### IMPORTANT

Before you move an Exchange mailbox from Exchange 2013 to Exchange 2010, the Exchange administrator must make sure that the Skype for Business Server administrator has first rolled back the Skype for Business Server user contacts from Exchange 2013 to Skype for Business Server. To roll back unified contact store contacts to Skype for Business Server, see procedure "To roll back unified contact store contacts from Exchange 2013 to Skype for Business Server," later in this section.

**How to roll back user contacts:** If you use the **Move-CsUser** cmdlet to move users between Skype for Business Server 2015 and Lync Server 2010, you can skip these steps because the **Move-CsUser** cmdlet automatically rolls back unified contact store when it moves users from Skype for Business Server 2015 to Lync Server 2010. **Move-CsUser** does not disable unified contact store policy, so the migration to unified contact store will recur if the user is moved back to Skype for Business Server 2015.

# Deploy Skype Connectivity in Skype for Business Server

8/19/2019 • 12 minutes to read

**Summary:** Learn how to connect Skype for Business Server with Skype consumer. Also known as Skype connectivity.

This article walks through deployment for Skype Connectivity.

## Skype Connectivity Overview for IT Professionals

Skype Connectivity provides Skype for Business users with the ability to search for and add Skype users. Skype Connectivity is a feature of Skype for Business that lets you enable federation and directory search with Skype users. After you enable Skype Connectivity your Skype for Business users will be able to search for and add Skype users.

## Skype Directory Search

Skype Directory Search functionality provides Skype for Business users with the ability to search for Skype contacts. The search functionality lets users search using the following:

- **Search by display name, example "John Doe"** - This could return many results, so you might not find what you are looking for.
- **Search by display name plus location, example "John Doe in Barcelona"** - This will narrow the results of the search down considerably.
- **Search by email, example "johndoe@outlook.com"** - This should return one result in most cases; the one that matches the specified email exactly. But if the same email is associated with more than one account, multiple results may be returned.
- **Search by phone number, example "123-123-1234"** - This should return one result in most cases; the one that matches the specified phone exactly. Phone number must include the country code (i.e. 1-xxx-yyy-zzzz). If the same phone number is associated with more than one account, multiple results may be returned.
- **Search by Skype Name, example "JohnDoe1456"** - If exact match is found, it will be returned as the first result. Other possible "name" matches may be returned.

### NOTE

Skype Directory Search must be able to communicate with the following IP addresses on port 443: 104.40.75.246, 23.101.135.34, and 40.113.86.19.

## Supported deployment matrix for Skype Directory Search

The following table outlines support for Skype Directory Search.

	SKYPE FOR BUSINESS SERVER FRONT END	LYNC SERVER 2013 (OR OLDER) FRONT END	COMMENTS
Skype for Business Server Edge	Supported	Not Supported	Skype for Business Server and Edge are prerequisites for Skype Directory Search
Skype for Business Server Edge + Lync Server 2013 Edge deployed side-by-side	Supported	Not Supported	Skype Directory Search traffic flows through Skype for Business Server Edge servers. Federation traffic goes through edge configured by the administrator. For example, the administrator could choose to continue to send federation traffic through Lync Server 2013 Edge servers which would not support Skype Directory Search.
Lync Server 2013 (or older) Edge	Not Supported	Not Supported	

**NOTE**

Addressbook service running on Skype for Business Server Front End finds the Edge by the existence of the Skype Search port 4443 in the Edge server.

**NOTE**

In case a customer has multiple sites in their on-premises deployment, and if they have deployed just one Skype for Business Server Edge server/pool, then Search traffic from all sites will go through the single available Edge server. The administrator needs to make sure the pools from all sites can access the deployed Skype for Business Server Edge server/pool.

**NOTE**

Skype graph service will throttle search requests from any on-premises or Office 365 customer if the request rate exceeds 15 requests / second.

**NOTE**

For large enterprise on-premises customers, the domains will need to be whitelisted with the Skype search service to allow higher request rates.

**NOTE**

Skype for Business Server will throttle incoming requests, if there are too many pending requests in the queue.

## Deploying Skype Connectivity for Skype for Business Online in Office

Skype Connectivity is also a feature of Skype for Business Online, which is part of Office 365. You can enable the Skype Connectivity feature from the Skype for Business Administration Center within the Office 365 portal.

For Office 365 Midsize Business, Office 365 Enterprise, Office 365 Education, and Office 365 for Government: Sign in to the Office 365 portal and navigate to the Skype for Business Administration Center. Go to External Communications. Under Public IM Service Providers, click Enable. If you want to control individual user access to Skype Connectivity, you can do so by editing individual users' External Communications settings.

For Office 365 Small Business Premium: Sign in to Office 365, and go to Admin > Service Settings > Instant messaging, meetings and conferencing. Turn on External communications. The External communications switch turns on both Skype Connectivity and communications with other organizations that use Skype for Business.

For more information about Skype for Business Online administration, see:

- [Allow users to contact external Skype for Business users](#)
- [What to try if you can't IM Skype for Business or Skype external contacts](#)
- [Add a contact in Skype for Business](#)
- [Admins: Configure Skype for Business settings for individual users](#)

## Deploying Skype Connectivity for Skype for Business Server

Skype for Business Server uses the federation access architecture to support connectivity with Skype. This connectivity enables your Skype for Business Server users to add Skype. Skype clients can also add Skype for Business users to their contact list. Based on policies administratively set in Skype for Business Server users will be able to communicate using instant messaging, see each other's presence, and initiate audio and video calls. Skype connectivity is also a feature of Skype for Business Online, and can be enabled for Skype for Business Online customers from the Skype for Business Administration Center within the Office 365 portal.

### NOTE

If Skype for Business Server is already configured to connect with Windows Messenger by using Public Instant Messaging Connectivity (PIC), your deployment is already configured for Skype connectivity. The only change you may want to consider is to rename your existing Messenger PIC entry as Skype.

### **The Skype for Business Server public IM connectivity provisioning site is no longer available**

The site that was formerly used to manually provision federation between Skype for Business on-premises deployments and Skype is no longer necessary and will be shut down on 8/15/2019. Federation with Skype now utilizes federated partner discovery, which is the same mechanism required for federation with Skype for Business Online.

Communication between any on-premises Skype for Business deployment and Skype users via the existing Public IM infrastructure now requires the on-premises Edge Server configuration to be compatible with Skype for Business Online.

### NOTE

No action is needed by most customers, including all deployments that federate with Skype for Business Online.

On-premises deployments are required to publish a Federation DNS SRV record for each domain that they host. Guidance is available in [DNS planning](#). Each domain must resolve by DNS SRV query to an edge server FQDN that satisfies a top-level suffix match of the domain. For example, consider the domain "contoso.com":

VALID FQDNS	COMMENT
sip.contoso.com	
sipfed.contoso.com	In each case, the exact FQDN must be present in either the SN or the SAN of the external certificate installed on the edge server.
access.contoso.com	
Invalid FQDNs	Reason
sip.contoso-edge.com	Not a suffix match.
sip.it.contoso.com	Not a top-level suffix match.

Further guidance regarding External Certificates can be found in [Certificate planning](#).

#### FAQs

**Why is the provisioning website being shut down?** The public IM (PIC) provisioning mechanism (pic.lync.com) that was deployed in 2006 is no longer serviceable and will be shut down on 8/15/2019. Instead, public IM federation will assume the same federation model used by Skype for Business Online, known as "partner discovery", whereby an on-premises deployment is publicly discoverable by its federation DNS SRV record(s).

**Does this change mean that Public IM federation is being deprecated?** No. Public IM federation will continue to be supported for many years, probably until the Skype for Business on-premises product reaches end-of-life.

**Our company has a hybrid relationship (shared address space) with Skype for Business Online, are we affected?** No, since you are already federating with Skype for Business Online, this change will not affect you.

**Does this change mean that our company has to enable federation with Skype for Business Online?** No. If your edge server proxy settings do not enable federation with the Skype for Business Online hosting provider (sipfed.online.lync.com) then this change will not affect that. However, the same DNS and certificate requirements that apply to federating with Skype for Business Online now also apply to federating with Skype users.

**Our company is large and cannot change its edge configuration due to regulatory/compliance/etc reasons ... what can we do?** Any on-premises organization that cannot change its edge server configuration as specified should reach out to product support at the earliest opportunity.

#### Enabling Federation and Public IM Connectivity (PIC)

Now focus on the Skype for Business Server environment and administrative tasks required to configure Skype Connectivity. In this section, we assume that the administrator has deployed Skype for Business Server and configured external access, also known as Edge servers.

There are three primary steps required to enable federation and PIC. These are:

1. Configure Federation and PIC
2. Configure at least one policy to support federated user access
3. Configure the Skype PIC provider setting

##### 1. Configure Federation and PIC

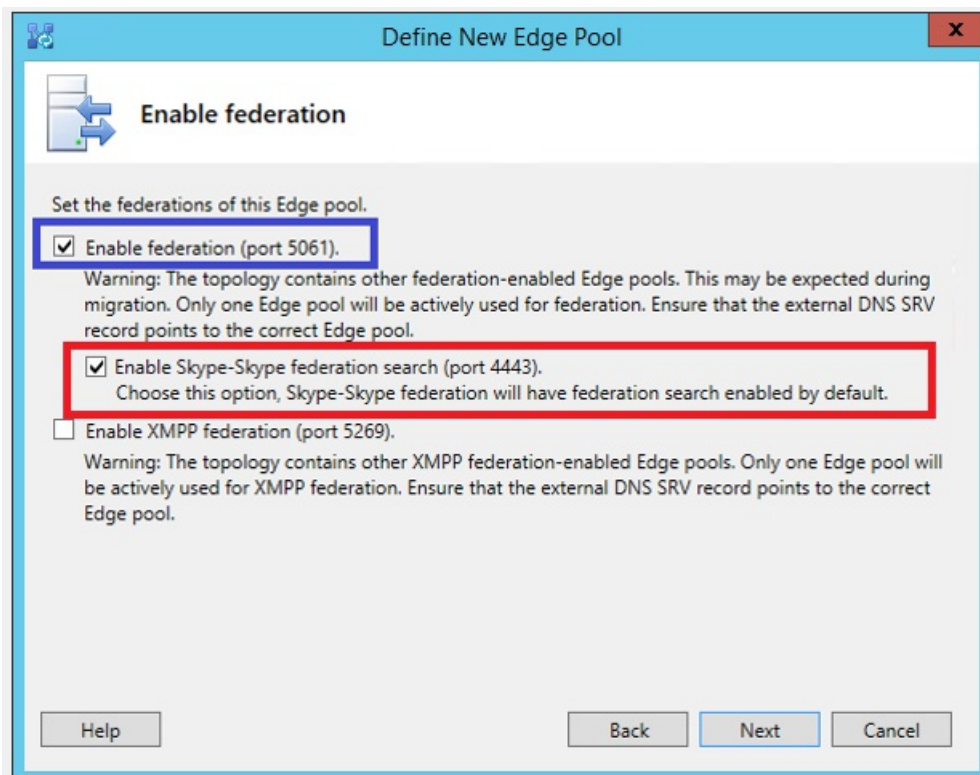
Federation is required to enable Skype users to communicate with Skype for Business users in your organization. Public Instant Messaging Connectivity (PIC) is a class of federation, and it must be configured to enable your

Skype for Business users to communicate with Skype users. Federation and PIC are configured by using the Skype for Business Server Control Panel.

**NOTE**

PIC federation is no longer supported by product releases prior to Lync Server 2010 (Live Communication Server, Office Communications Server). The supported platforms for PIC federation include Skype for Business Server, Lync Server 2013, and Lync Server 2010.

Federation is required to enable Skype users to communicate with Skype for Business users in your organization. Public Instant Messaging Connectivity (PIC) is a class of federation, and it must be configured to enable your Skype for Business Server users to communicate with Skype users. Federation and PIC are configured by using the Edge configuration dialog of the Skype for Business Server Control Panel as shown in the figure.



**NOTE**

EnableSkypeIdRouting and EnableSkypeDirectorySearch attributes need to be set to true in the public provider settings (see later instructions) for Search to work.

This completes the administrative tasks that must be performed on the server. You are now set up for Skype Connectivity.

**2. Configure at least one policy to support federated user access**

Using the Skype for Business Server Control Panel, an administrator must configure one or more external user access policies to control whether Skype users can collaborate with internal Skype for Business Server users.

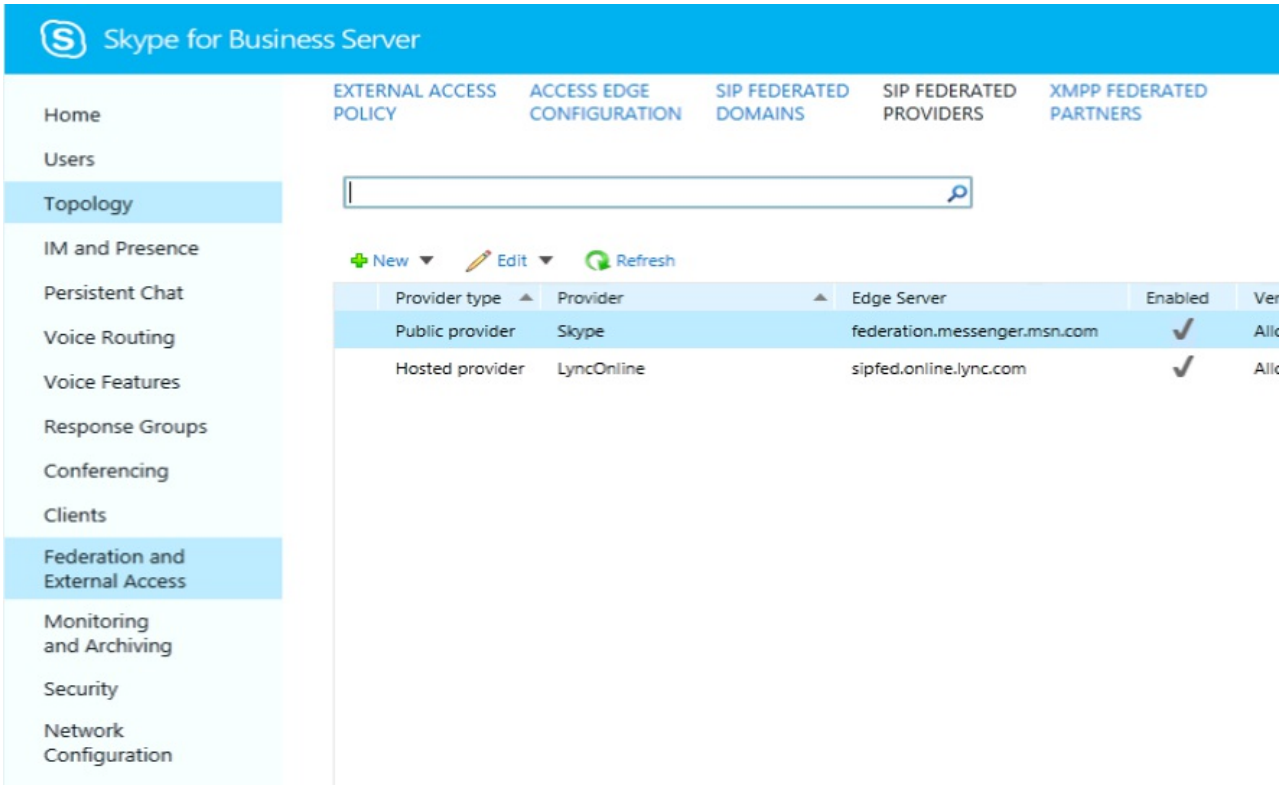
**3. Configure the Skype PIC provider setting**

Using the Skype for Business Server Management Shell, an administrator must configure the Skype for Business client policy to display Skype as an additional PIC provider.

**NOTE**

Users of the Public Instant Messaging Connectivity (PIC) service providers can't participate in IM or conferences in your organization until you also configure at least one policy (step 2, earlier in this procedure) to support public IM connectivity.

For new installations you can configure Skype Connectivity by enabling a Skype Public Provider using the Skype for Business Server Control Panel as shown in the figure.



**NOTE**

To configure Skype Connectivity when upgrading to Skype for Business Server you must remove and re-add the existing Skype public provider.

Configuring Skype Connectivity can also be done using only PowerShell. To configure Skype Connectivity using PowerShell:

1. From a Skype for Business Server Front End Server, open the Skype for Business Server Management Shell.
2. Run the following two commands:

```
Remove-CsPublicProvider -Identity <identity-name>
```

**NOTE**

If you do not already have a PIC provider in your environment and are creating a new PIC provider then you do not need to run the Remove-CsPublicProvider cmdlet.



```
New-CsPublicProvider -Identity Skype -ProxyFqdn federation.messenger.msn.com -IconUrl
https://images.edge.messenger.live.com/Messenger_16x16.png -NameDecorationRoutingDomain msn.com -
NameDecorationExcludedDomainList "msn.com,outlook.com,live.com,hotmail.com" -Enabled $true -
EnableSkypeIdRouting $true -EnableSkypeDirectorySearch $true
```

What do the less obvious parameters do?

- ProxyFqdn: location of Skype federation edge (owned/maintained by Microsoft)
- IconURL: icon used by Lync & Skype for Business client to visually identify Skype contacts
- NameDecorationRoutingDomain and NameDecorationExcludedDomainList: setting these allows users to enter Skype users' MSAs without needing to know about "decorating" non-Microsoft domains with "msn.com". This eliminates the need to type "user(contoso.com)@msn.com" for all domains that are NOT in the ExcludedDomainList. The SfB client will automatically format the MSA if the domain is NOT in the Excluded list. We've added the most common Microsoft Account domains to the excluded list.

#### NOTE

Public Provider must be removed and added new if changes are made. No in-place changes are allowed.

#### NOTE

Added in Lync Server 2013 CU5 & Lync desktop client in Office 2013 SP1, the NameDecorationRoutingDomain and NameDecorationExcludedDomainList improve the situation where Lync users adding Skype contacts needed to "decorate" non-Microsoft domains to identify and route them to Skype (the format of: user(contoso.com)@msn.com). These new settings will allow automatic formatting of the address user's enter in the "Add Skype contact" dialog box with the NameDecorationRoutingDomain (which should be set to msn.com) if it does not contain the domains in the NameDecorationExcludedDomainList (we currently can support msn.com, live.com, Hotmail.com, outlook.com).

3. From a Skype for Business client users can now search for and add a Skype user.

## Clients and Interoperability Matrix

The following table outlines the status of interop between the latest version of Skype consumer and the latest version of Skype for Business.

SKYPE CLIENTS	ADD CONTACTS, IM, PRESENCE, AUDIO, AND VIDEO CALLING	COMMENT
Skype Windows Desktop	7.6 or higher, Windows XP and higher	<b>NEW:</b> Support added for Windows Skype client running on Windows XP, and Windows Vista ( <b>requires latest client version 7.26 or higher</b> )
Skype Mobile - Android Phone and Tablet	6.19 or higher, running Android OS version 4.0.3 or higher	Low spec devices may not support video calling
Skype Mobile - iOS	6.11 or higher, on IOS 7 or higher	Not supported are iPhone 4 and earlier, iPod 4th generation and earlier, iPad 1st generation

<b>SKYPE CLIENTS</b>	<b>ADD CONTACTS, IM, PRESENCE, AUDIO, AND VIDEO CALLING</b>	<b>COMMENT</b>
Skype Mac	7.19 or higher, on Mac OS X 10.9 (Mavericks) or higher	Requires Mac OSX 10.9 or higher
Skype Universal Windows App (Windows 10) Desktop and Mobile	Windows 10 (Redstone 1 update or later)	Windows Universal App will receive update in Fall 2016 adding interop support

The following table outlines the status of interop between the latest version of Skype for Business and the latest version of Skype consumer.

<b>CLIENT</b>	<b>SKYPE DIRECTORY SEARCH AND ADD CONTACTS</b>	<b>SKYPE A/V, IM INTEROP</b>
Skype for Business	Yes	Yes
Skype for Business on Mac	Can add (no search)	Yes
Lync Desktop 2013	Can add (no search)	Yes
Lync Web App - online and on-premises	N/A	N/A
Lync Mobile - Windows Phone	Coming Soon	Yes
Lync Mobile - Android	Coming Soon	Yes
Lync Mobile - iOS	Coming Soon	Yes
Lync Room System	Coming Soon	Yes
Lync Modern App (Win 8.1)	Yes	Yes
Lync Mac 2011	Can add (no search)	Yes
Lync Desktop 2010	Can add (no search)	Yes
Lync Phone Edition	N/A	N/A
Lync Attendant	N/A	N/A

# Deploy conferencing in Skype for Business Server

8/7/2019 • 9 minutes to read

**Summary:** Read this topic to learn how to deploy conferencing in Skype for Business Server.

There are four types of conferencing available in Skype for Business Server: web conferencing, audio and video (A/V) conferencing, dial-in conferencing, and instant message (IM) conferencing. You can choose to enable all conferencing types, or to use only one type, depending on your needs.

When you deploy Skype for Business Server, IM conferencing capabilities are automatically deployed. When you create and publish a new topology by using Topology Builder, you specify whether to deploy web, A/V, and dial-in conferencing, as described in the following checklists:

- [Deployment checklist for web and audio/video conferencing](#)
- [Deployment flowchart and checklist for dial-in conferencing](#)

Before you deploy conferencing, you should read the following planning topics:

- [Plan for conferencing in Skype for Business Server](#)
- [Hardware and software requirements for conferencing in Skype for Business Server](#)
- [Plan your conferencing topology for Skype for Business Server](#)
- [Plan for dial-in conferencing in Skype for Business Server](#)
- [Plan for large meetings in Skype for Business Server](#)

## Deployment checklist for web and audio/video conferencing

The following table provides an overview of the steps required to deploy web and audio/video conferencing into an existing topology. Links to the associated planning and procedural documentation are included.

PHASE	STEPS	ROLES AND GROUP MEMBERSHIPS	DOCUMENTATION
-------	-------	-----------------------------	---------------

PHASE	STEPS	ROLES AND GROUP MEMBERSHIPS	DOCUMENTATION
<p><b>Install required hardware and software</b></p>	<p>Conferencing runs on Front End Servers of a Front End pool and Standard Edition servers. See the server and environmental requirements for Front End Servers.</p> <p>If you are enabling web conferencing, you will need to ensure that Skype for Business Server can communicate with Office Web Apps Server, which is used to handle sharing and rendering of PowerPoint presentations.</p> <p>For web conferencing, you also need to specify a file share to be used as the file store.</p> <p>Do you want to enable external users with Skype for Business clients to join conferences? If so, you need to deploy Edge Servers.</p>	<p>Domain user who is a member of the local Administrators group</p>	<p><a href="#">Server requirements for Skype for Business Server 2019</a></p> <p><a href="#">Server requirements for Skype for Business Server 2015</a></p> <p><a href="#">Environmental requirements for Skype for Business Server 2015</a></p> <p><a href="#">Hardware and software requirements for conferencing in Skype for Business Server</a></p> <p><a href="#">Configure integration with Office Web Apps Server in Skype for Business Server</a></p> <p><a href="#">Create a file share in Skype for Business Server</a></p> <p><a href="#">Plan for Edge Server deployments in Skype for Business Server 2015</a></p> <p><a href="#">Deploy Edge Server in Skype for Business Server 2015</a></p>
<p><b>Create the appropriate internal topology to support conferencing</b></p>	<p>You need to run Topology Builder to add conferencing to the topology, and then publish the topology.</p>	<p>To define a topology, an account that is a member of the local Users group</p> <p>To publish the topology, an account that is a member of the Domain Admins group and RTCUniversalServerAdmins group, and that has full control permissions (read/write/modify) on the file share to be used for the Skype for Business Server file store (so that Topology Builder can configure the required DACLs)</p>	<p><a href="#">Create and publish new topology in Skype for Business Server</a></p>
<p><b>Configure conferencing policies and configuration settings</b></p>	<p>Use Skype for Business Server Control Panel or Skype for Business Server Management Shell to configure conferencing policies and configuration settings.</p>	<p>RTCUniversalServerAdmins group (Windows PowerShell only) or assign users to the CSAdministrator role</p>	<p><a href="#">Manage conferencing policies in Skype for Business Server</a></p> <p><a href="#">Manage meeting configuration settings in Skype for Business Server</a></p> <p><a href="#">New-CsConferencingPolicy</a></p> <p><a href="#">Set-CsConferencingPolicy</a></p> <p><a href="#">New-CsConferencingConfiguration</a></p> <p><a href="#">Set-CsConferencingConfiguration</a></p> <p><a href="#">New-CsMeetingConfiguration</a></p> <p><a href="#">Set-CsMeetingConfiguration</a></p>

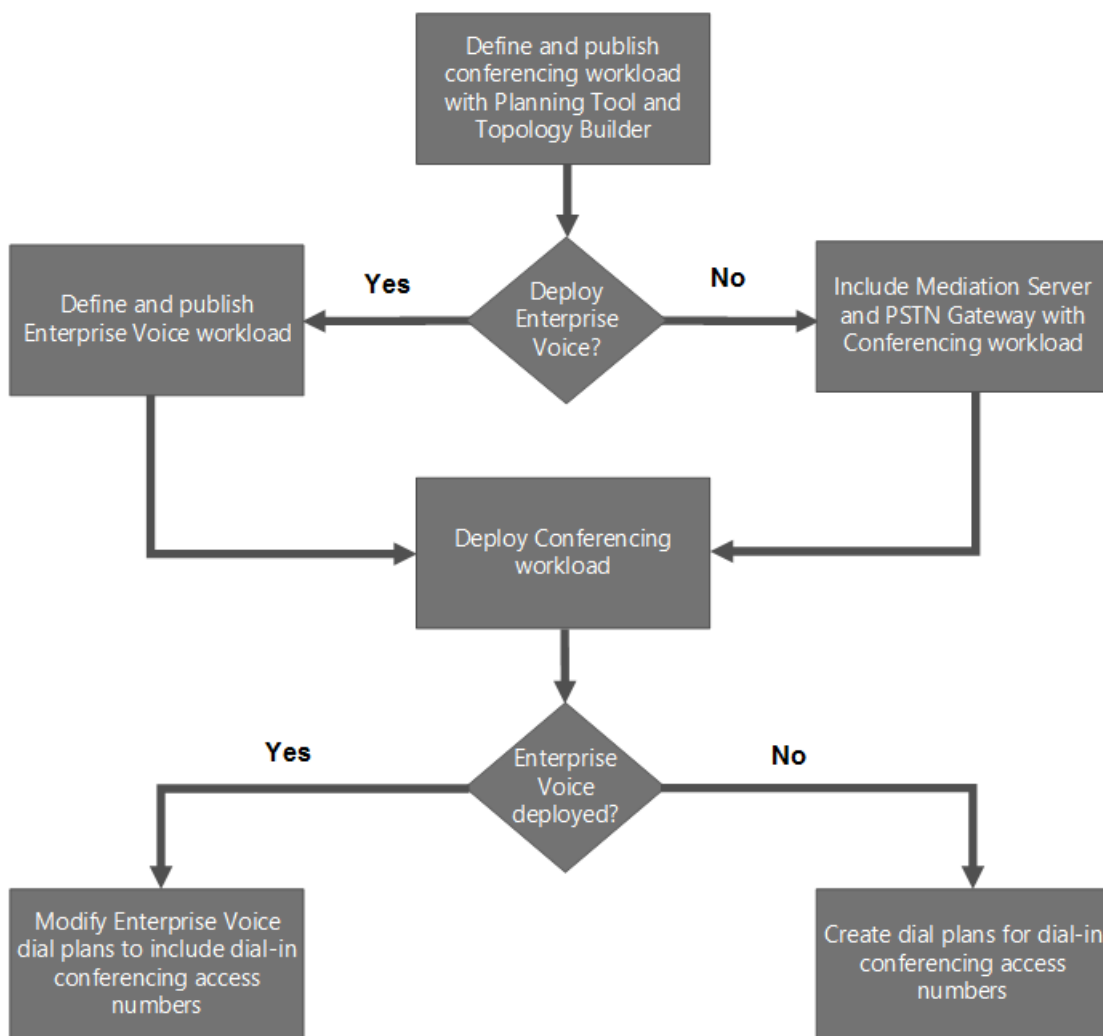
# Deployment flowchart and checklist for dial-in conferencing

Dial-in conferencing allows users to dial in from the public switched telephone network (PSTN) to join an audio/video conference.

Some of the components required for dial-in conferencing are also used for Enterprise Voice. For example, if you are deploying Enterprise Voice, you must also deploy a Mediation Server and a PSTN gateway--components that are also required for dial-in conferencing. How you deploy dial-in conferencing, therefore, depends on whether you are also deploying an Enterprise Voice solution.

The dial-in conferencing flowchart shows the steps you must follow depending on whether you are also deploying an Enterprise Voice solution. The table following the flowchart provides an overview of steps required and recommended for deploying dial-in conferencing. Links to the associated planning and procedural documentation are also included. For more information about planning a complete Enterprise Voice solution, see [Plan your Enterprise Voice solution in Skype for Business Server](#).

## Dial-in conferencing flowchart



## Dial-in conferencing deployment checklist

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
-------	-------	----------------------------	---------------

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
<p><b>Install required hardware and software</b></p>	<p>Conferencing runs on Front End Servers of a Front End pool and Standard Edition servers. See the server and environmental requirements for Front End Servers. You need to ensure that the following are installed before configuring dial-in conferencing:</p> <ul style="list-style-type: none"> <li>Mediation Server</li> <li>PSTN gateway</li> <li>Unified Communications Application Service (UCAS) (called the Application service)</li> <li>Conferencing Attendant application</li> <li>Conferencing Announcement application</li> </ul>	<p>Domain user who is a member of the local Administrators group</p>	<p><a href="#">Server requirements for Skype for Business Server 2015</a></p> <p><a href="#">Environmental requirements for Skype for Business Server 2015</a></p> <p><a href="#">Hardware and software requirements for conferencing in Skype for Business Server</a></p> <p><a href="#">Plan for dial-in conferencing in Skype for Business Server Mediation Server component in Skype for Business Server</a></p> <p><a href="#">Deploy a Mediation Server in Topology Builder in Skype for Business Server</a></p> <p><a href="#">Define a gateway in Topology Builder in Skype for Business Server</a></p>
<p><b>Create a topology that includes the Conferencing workload, including a Mediation Server and PSTN gateway, and deploy the Front End pool or Standard Edition server</b></p>	<ol style="list-style-type: none"> <li>1. Run Topology Builder to configure your topology. While configuring the topology, select the dial-in conferencing option.</li> <li>2. Publish the topology and deploy the Front End pool or Standard Edition server.</li> <li>3. If necessary, create a stand-alone Mediation Server and associate it with a PSTN gateway.</li> </ol> <p><b>Note:</b> This step is required only if you do not deploy Enterprise Voice and do not collocate the Mediation Server with the Enterprise Edition Front End Server or Standard Edition server. If you deploy Enterprise Voice, you install and configure Mediation Servers and PSTN gateways as part of the Enterprise Voice deployment. If you collocate the Mediation Server, you install and configure the Mediation Server as part of the Front End pool or Standard Edition server deployment.</p>	<p>Domain Admins RTCUniversalServerAdmins Administrator</p>	<p><a href="#">Create and publish new topology in Skype for Business Server</a></p> <p><a href="#">Deploy a Mediation Server in Topology Builder in Skype for Business Server</a></p> <p><a href="#">Define a gateway in Topology Builder in Skype for Business Server</a></p>

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
<p><b>Configure dial plans</b></p>	<p>A dial plan is a set of phone number normalization rules that translate phone numbers dialed from a specific location to a single standard (E.164) format for purposes of phone authorization and call routing. The same phone number dialed from different locations can, based on the respective dial plans, resolve to different E.164 numbers, as appropriate to each location. If you deploy Enterprise Voice, you set up dial plans as part of that deployment, and you need to make sure that the dial plans also accommodate dial-in conferencing. If you do not deploy Enterprise Voice, you need to set up dial plans for dial-in conferencing. Use Skype for Business Server Control Panel or Skype for Business Server Management Shell to set up dial plans as follows:</p> <ol style="list-style-type: none"> <li>1. Create one or more dial plans for routing dial-in access phone numbers.</li> <li>2. Assign a default dial plan to each pool. Set the <b>Dial-in conferencing region</b> to the geographic location to which the dial plan applies. The region associates the dial plan with dial-in access numbers.</li> </ol>	<p>RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator</p>	<p><a href="#">Configure dial-in conferencing in Skype for Business Server</a> <a href="#">Create or modify a dial plan in Skype for Business Server</a> <a href="#">New-CsDialPlan</a></p>
<p><b>Make sure that dial plans are assigned regions</b></p>	<p>Run the <b>Get-CsDialPlan</b> and <b>Set-CsDialPlan</b> cmdlets to make sure that all dial plans have a region assigned.</p>	<p>RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator</p>	<p><a href="#">Configure dial-in conferencing in Skype for Business Server</a> <a href="#">Create or modify a dial plan in Skype for Business Server</a> <a href="#">Get-CsDialPlan</a> <a href="#">Set-CsDialPlan</a></p>

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
<p><b>Configure conferencing policy to support dial-in conferencing</b></p>	<p>Use Skype for Business Server Control Panel or Skype for Business Server Management Shell to configure <b>Conferencing Policy</b> settings. Specify whether:</p> <ul style="list-style-type: none"> <li>PSTN conference dial-in is enabled.</li> <li>Users can invite anonymous participants.</li> <li>Unauthenticated users can join a conference by using dial-out phoning. With dial-out phoning, the conference server calls the user, and the user answers the phone to join the conference.</li> </ul>	<p>RTCUniversalServerAdmins CsServerAdministrator CsAdministrator</p>	<p><a href="#">Manage conferencing policies in Skype for Business Server</a> <a href="#">New-CsConferencingPolicy</a> <a href="#">Set-CsConferencingPolicy</a></p>
<p><b>Configure dial-in access numbers</b></p>	<p>Use Skype for Business Server Control Panel or Skype for Business Server Management Shell to set up dial-in access numbers that users call to dial in to a conference, and specify the regions that associate the access number with the appropriate dial plans. The first three access numbers for the region specified by the organizer's dial plan are included in the conference invitation. All access numbers are available on the Dial-in Conferencing Settings page.</p> <p><b>Note:</b> After you create dial-in access numbers, you can use the <b>Set-CsDialInConferencingAccessNumber</b> cmdlet to modify the display name of the Active Directory contact objects so that users can more easily identify the correct access number.</p>	<p>RTCUniversalServerAdmins CsServerAdministrator CsAdministrator</p>	<p><a href="#">Create or modify a dial plan in Skype for Business Server</a> <a href="#">Manage dial-in conferencing access numbers in Skype for Business Server</a> <a href="#">New-CsDialInConferencingAccessNumber</a> <a href="#">Set-CsDialInConferencingAccessNumber</a></p>
<p><b>Assign a Line URI to a user account</b></p>	<p>Use Skype for Business Server Control Panel or Skype for Business Server Management Shell to configure the telephony <b>Line URI</b> as a unique, normalized phone number (for example, tel:+14255550200).</p>	<p>RTCUniversalServerAdmins CsAdministrator CsUserAdministrator</p>	<p><a href="#">Assign a Line URI to a user account</a></p>



PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
<b>(Optional) Verify or modify user personal identification number (PIN) requirements</b>	Use Skype for Business Server Control Panel or Skype for Business Server Management Shell to view or modify the Conferencing <b>PIN Policy</b> . You can specify minimum PIN length, maximum number of logon attempts, PIN expiration, and whether common patterns are allowable.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	<a href="#">Manage PIN policies for dial-in conferencing in Skype for Business Server</a> <a href="#">Get-CsPinPolicy</a> <a href="#">Set-CsPinPolicy</a>
<b>(Optional) Modify key mapping of DTMF commands</b>	Use the <b>Set-CsDialInConferencingDtmfConfiguration</b> cmdlet to modify the keys used for dual-tone multi-frequency (DTMF) commands, which participants can use to control conference settings (such as mute and unmute or lock and unlock).	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	<a href="#">Manage key mapping for DTMF commands in Skype for Business Server</a> <a href="#">Set-CsDialInConferencingDtmfConfiguration</a>
<b>(Optional) Modify conference join and leave announcement behavior</b>	Use the <b>Set-CsDialInConferencingConfiguration</b> to change how announcements work when participants join and leave conferences.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	<a href="#">Manage conference join and leave announcements in Skype for Business Server</a> <a href="#">Set-CsDialInConferencingConfiguration</a>
<b>(Recommended) Configure conference directories</b>	Use the <b>New-CsConferenceDirectory</b> cmdlet to create one conference directory for every 999 users in the pool.	RTCUniversalServerAdmins	<a href="#">(Recommended) Create Conference Directories</a> <a href="#">New-CsConferenceDirectory</a>
<b>(Optional) Verify dial-in conferencing settings</b>	Use the <b>Get-CsDialInConferencingAccessNumber</b> cmdlet to search for dial plans that have a dial-in conferencing region that is not used by any access number and for access numbers that have no region assigned.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator CsViewOnlyAdministrator CsHelpDesk	<a href="#">Configure dial-in conferencing in Skype for Business Server</a> <a href="#">Test dial-in conferencing in Skype for Business Server</a> <a href="#">Get-CsDialInConferencingAccessNumber</a>
<b>(Optional) Verify dial-in conferencing</b>	Use the <b>Test-CsDialInConferencing</b> cmdlet to test that the access numbers for the specified pool work correctly.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	<a href="#">Test dial-in conferencing in Skype for Business Server</a> <a href="#">Test-CsDialInConferencing</a>

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
<p><b>(Optional) Welcome users to dial-in conferencing and set the initial PIN</b></p>	<p>Use the <b>Set-CsPinSendCAWelcomeMail</b> script to set users' initial PINs and send a welcome email that contains the initial PIN and a link to the Dial-in Conferencing Settings page.</p>	<p>RTCUniversalServerAdmins</p>	<p><a href="#">Send welcome email to dial-in users in Skype for Business Server</a></p>

# Configure integration with Office Web Apps Server in Skype for Business Server

8/7/2019 • 5 minutes to read

**Summary:** Read this topic to learn how to configure integration between Office Web Apps Server and Skype for Business Server to enable PowerPoint presentations for web conferencing.

Skype for Business Server employs Office Web Apps Server to handle PowerPoint presentations for web conferencing. For information about the advantages to this approach, see [Plan for conferencing in Skype for Business Server](#).

Before you can configure Skype for Business Server to use Office Web Apps Server, you must ensure that Office Web Apps Server is already deployed and configured. For information on Office Web Apps Server, see the article [Deploy the infrastructure: Office Online Server](#).

After Office Web Apps Server has been successfully installed and your Web farm correctly configured, you must then configure Skype for Business Server to communicate with the new server by adding the Office Web Apps Server discovery URL to your Skype for Business Server topology.

## NOTE

The latest iteration of Office Web Apps Server is named Office Online Server, which is supported by Skype for Business Server. For more detail, refer to the [Office Online Server documentation](#).

## Configure Skype for Business Server to communicate with Office Web Apps Server

To add Office Web Apps Server to your topology, complete the following steps:

1. Open Skype for Business Server Topology Builder.
2. In the **Topology Builder** dialog box, select **Download Topology from existing deployment** and then click **OK**.
3. In the **Save Topology As** dialog box, type a name for your topology document (for example, **PreWebAppsServerTopology**) in the **File name** box and then click **Save**. This topology can later be retrieved and republished if you encounter problems with your new topology.
4. In Topology Builder, expand **Skype for Business Server**, expand the name of your site, expand **Enterprise Edition Front End pools**, right-click the name of one of your pools, and then click **Edit Properties**.
5. In the **Edit Properties** dialog box, on the **General** tab, find the heading **Associate Office Web Apps Server** and then click **New** (or select an existing Office Web Apps Server from the drop-down list).
6. In the **Define New Office Web Apps Server** dialog box, type the fully qualified domain name (FQDN) of your Office Web Apps Server computer in the **Office Web Apps Server FQDN** box; when you do this, your Office Web Apps Server discovery URL should automatically be entered into the **Office Web Apps Server discovery URL** box.
  - If the Office Web Apps Server is installed on-premises and in the same network zone as Skype for

Business Server then the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)** should not be selected.

- If the Office Web Apps Server is deployed outside your internal firewall, then select the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)**.

7. In the **Define New Office Web Apps Server** dialog box, click **OK**, and then click **OK** in the **Edit Properties** dialog box. The discovery URL will then be listed as one of the pool's Associations.

You will have to repeat this process for each pool that needs to be associated with your Office Web Apps Server.

After you have added the discovery URL to the topology, you must then publish the updated topology. To do that in Topology Builder:

1. Click **Action** and then click **Publish Topology**.
2. In the Publish Topology wizard, on the **Publish the Topology** page, click **Next**.
3. On the **Publishing wizard complete** page, click **Finish**.
4. Close Topology Builder.

## Configure access for external users

If you want external users (that is, users logging on from outside your organization's firewall) to have access to Office Web Apps Server PowerPoint presentations, then you will need to use Office Web Apps Server and a reverse proxy server. You will also need to create and configure a website publishing rule, which will help ensure that users are able to connect to the server.

## Validate the configuration

After Office Web Apps Server has been added to the topology, and after that topology has been published, you should see two new event log events in the Skype for Business Server event log. First, an LS Data MCU event (event ID 41034) should be added; this event will report that the Office Web Apps Server has been discovered:

**Web Conferencing Server Office Web Apps Server is discovered, PowerPoint content is enabled.**

In addition to that you should see another LS Data MCU event (event ID 41032) that reports back Office Web Apps Server URLs. For example, you should see something similar to this:

**Web Conferencing Server Office Web Apps Server discovery has succeeded.**

**Office Web Apps Server internal presenter page:** <https://atl-officewebapps-001.litwareinc.com/m/Presenter.aspx?a=0&embed=>

**Office Web Apps Server internal attendee page:** <https://atl-officewebapps-001.litwareinc.com/m/ParticipantFrame.aspx?a=0&embed=true&=>

If you have configured access for external users, you will also see something similar to:

**Office Web Apps Server external presenter page:** <https://atl-officewebapps-001.litwareinc.com/m/Presenter.aspx?a=0&embed>

**Office Web Apps Server internal attendee page:** <https://atl-officewebapps-001.litwareinc.com/m/ParticipantFrame.aspx?a=0&embed=true&=>

If you see an LS Data MCU event with the event ID of 41033 that means that Office Web Apps Server discovery has failed. In that case, Skype for Business Server will try as many times as needed to discover the newly-configured Office Web Apps Server. If the discovery process fails repeatedly you should remove Office Web Apps Server from your topology document, publish the updated topology, and then try adding Office Web Apps

Server back to the topology after the connectivity issues have been resolved.

If Office Web Apps Server appears to be configured correctly and has been recognized by the discovery process you can verify that Office Web Apps Server is working as expected by sharing a PowerPoint presentation between a pair of Skype for Business clients. If User A can load and display the PowerPoint presentation and if User B can then join the meeting and see that presentation then Office Web Apps Server is working.

Even if Office Web Apps Server appears to be configured correctly, you could potentially receive the error message "Some sharing features are unavailable due to server connectivity issues" when you try sharing a PowerPoint presentation. If you receive that error message you should restart the Front End server (or servers) associated with the new Office Web Apps Server.

# Configure dial-in conferencing in Skype for Business Server

8/7/2019 • 9 minutes to read

**Summary:** Read this topic to learn how to configure dial-in conferencing in Skype for Business Server.

After you have created a topology that includes the conferencing workload and selected dial-in conferencing, you must perform additional steps to configure dial-in conferencing. Before you read this topic, be sure you have read [Plan for dial-in conferencing in Skype for Business Server](#), [Hardware and software requirements for conferencing in Skype for Business Server](#), and the [Deployment flowchart and checklist for dial-in conferencing](#).

To configure dial-in conferencing, you must perform the following tasks:

- [Configure dial plans](#)
- [Configure dial-in conferencing regions](#)
- [Configure dial-in access numbers](#)
- [Configure conferencing policies](#)
- [Assign a Line URI to a user account](#)

In addition, you may perform the following optional tasks. For more information about these optional tasks, see [Manage dial-in conferencing in Skype for Business Server](#).

- Manage PIN policies for dial-in conferencing
- Manage key mapping for DTMF commands
- Create conference directories
- Manage conference join and leave announcements
- Test dial-in conferencing settings
- Send welcome mail to dial-in users

## Configure dial plans

When you deploy dial-in conferencing, you need to create or modify one or more dial plans for routing dial-in access phone numbers. You must also make sure that each dial plan contains at least one normalization rule--a rule that converts telephone extensions into complete phone numbers in E.164 format.

Users of dial-in conferencing join conferences as authenticated enterprise users by entering their personal identification number (PIN) and their phone number. You need a normalization rule to convert extensions into complete phone numbers so that users can be authenticated when they enter just a telephone extension.

To set up dial plans for dial-in conferencing:

- Whether or not you deploy Enterprise Voice, modify the global dial plan to add a dial-in conferencing region and to make sure that a normalization rule accurately converts your dial-in access numbers. For detailed instructions, see [Create or modify a dial plan in Skype for Business Server](#).
- If you did not deploy Enterprise Voice, create dial plans for your dial-in conferencing access numbers. Be sure to include a dial-in conferencing region. For detailed instructions, see [Create or modify a dial plan in](#)

[Skype for Business Server](#).

- If you deployed Enterprise Voice, modify Enterprise Voice dial plans as necessary to include regions and use appropriate normalization rules for dial-in access numbers. You can also create dedicated dial plans that are used only for dial-in access numbers. For detailed instructions, see [Create or modify a dial plan in Skype for Business Server](#).

For details about creating normalization rules, see [Create or modify a normalization rule in Skype for Business](#).

## Configure dial-in conferencing regions

When you set up a dial plan, you specify the dial-in conferencing region that applies to that dial plan. The dial-in conferencing region associates dial-in conferencing access numbers with the appropriate dial plan. When you create the dial-in access number, you select the regions that associate the access number with the appropriate dial plans.

Because it is important to specify a region for all dial plans, we recommend that you verify that all dial plans have conferencing regions.

To verify whether the region is set for all dial-in conferencing dial plans, use the **Get-CsDialPlan** cmdlet. If the region is missing from dial plans, you can use the **Set-CsDialPlan** cmdlet to set the region. You can also use Skype for Business Server Control Panel to update the region in existing dial plans. For details about using Skype for Business Server Control Panel, see [Create or modify a dial plan in Skype for Business Server](#).

### To verify whether dial plans have the region property set

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-VoiceAdministrator**, **Cs-ServerAdministrator**, or **CsAdministrator** role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialPlan [-Identity <Identifier of the dial plans to be retrieved>]
```

For example:

```
Get-CsDialPlan
```

In this example, all the dial plans configured for your organization are returned.

4. Review the returned dial plans to identify any that are missing the dial-in conferencing region.

For more information, see [Get-CsDialPlan](#).

### To set the region property for a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-VoiceAdministrator**, **Cs-ServerAdministrator**, or **CsAdministrator** role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. For any dial plans that are missing the dial-in conferencing region, run:

```
Set-CsDialPlan [-Identity <Identity of the dial plan to be modified>] -DialInConferencingRegion "<new region>"
```

For example:

```
Set-CsDialPlan -Identity Redmond -DialInConferencingRegion "US West Coast"
```

In this example, the dial plan with the Identity of Redmond is modified to set the DialInConferencingRegion property to "US West Coast".

For more information, see [Set-CsDialPlan](#).

## Configure dial-in access numbers

When you deploy dial-in conferencing, you need to set up phone numbers that users can dial from the public switched telephone network (PSTN) to join the audio portion of conferences. These dial-in access numbers appear in meeting invitations and on the Dial-in Conferencing Settings webpage.

Before you can create dial-in access numbers, you must first plan your dial-in conferencing regions and then configure dial plans with the regions. For details about regions, see [Plan for dial-in conferencing in Skype for Business Server](#). For details about configuring dial plans for dial-in conferencing, see [Create or modify a dial plan in Skype for Business Server](#).

### NOTE

You cannot use a new dial-in access number until Active Directory Domain Services (AD DS) replication of that access number is complete. Replication can take several hours to complete.

### NOTE

After you create dial-in access numbers, you can modify the display name for the Active Directory contact objects so that users can more easily identify the correct access number. To modify the display name, use the [Set-CsDialInConferencingAccessNumber](#) cmdlet. You should not modify Active Directory objects manually.

### To create a dial-in access number

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing** and then click **Dial-in Access Number**.
4. On the **Dial-in Access Number** page, do one of the following:
  - Click **New** to open **New Dial-in Access Number**.
  - Click one of the dial-in access numbers in the list, click **Edit**, and then click **Show details**.

### NOTE

Using the search field to search for the contents of a column in the list of dial-in access numbers may not yield the results you expect. Instead, sort the list by the column of interest to identify the dial-in access number you want to view or change.



5. In **Display number**, type the phone number that public switched telephone network (PSTN) phone users dial to join a conference. This number is displayed in meeting invitations and on the Dial-in Conferencing Settings webpage.
6. In **Display name**, type a description for the dial-in access number. This is the name that is associated with the dial-in access number in Skype for Business search results. This name is displayed in the client when a user calls the access number.
7. In **Line URI**, type the E.164 number of the dial-in access number in TEL URI format, including the + symbol before the number and excluding spaces. For example, tel:+14255550200.

**NOTE**

The same Line URI cannot be reused by another dial-in conferencing access number.

8. In **SIP URI**, do the following:
  - In the text box, type a unique SIP URI for this dial-in conferencing access number. This SIP URI is displayed in various locations including, but not limited to, call notification messages and previous versions of Lync clients.

**NOTE**

The same SIP URI cannot be reused by another dial-in conferencing access number. The SIP URI cannot be modified after the access number is created. The only way to change the SIP URI is to delete and recreate the access number.

- In the drop-down list box, click the domain of the Conferencing Attendant application that supports this dial-in access number.
9. In **Pool**, click the pool that is running the instance of Conferencing Attendant that supports this dial-in access number.

**NOTE**

If you need to change the pool after you create the access number, you must use the [Move-CsApplicationEndpoint](#) cmdlet or delete and recreate the access number.

10. In **Primary language**, click the language in which prompts are played for this dial-in access number.

The primary language is the language that the Conferencing Attendant uses to answer the call. Supported languages are displayed alongside each access phone number on the Dial-in Conferencing Settings webpage.
11. (Optional) In **Secondary languages (maximum of four)**, click **Add**, select one or more additional languages that you want to support for callers to this dial-in access number, and then click **OK**.

You can choose up to four secondary languages for each dial-in access number. Users can select a secondary language before entering the conference ID when they dial in to a conference.
12. To add a region for the dial-in access number, under **Associated regions**, click **Add**, click one or more regions that are associated with the dial plans for this dial-in access number, and then click **OK**.
13. To delete a region from the dial-in access number, under **Associated regions**, click the region you want to delete, and then click **Remove**.

14. Click **Commit**.

## Configure conferencing policies

Conferencing policy is a user account setting that specifies the conferencing experience for participants. You can create conferencing policies with a site scope or a user scope. Conferencing policy settings encompass many aspects of conference scheduling and participation. Several conferencing policy settings support dial-in conferencing for participants. When you configure dial-in conferencing, you should verify that these fields are set appropriately for your organization, and modify them as necessary.

For more information about configuring conferencing policies, see [Manage conferencing policies in Skype for Business Server](#).

## Assign a Line URI to a user account

Dial-in users enter their phone number or extension and a PIN to join conferences as authenticated users. The telephony **Line URI** specified on Skype for Business Server user accounts is required for authentication.

The procedure in this topic describes how to assign a **Line URI** for a single user account. If you need to assign a **Line URI** for multiple user accounts, you can create a script that uses the **Set-CsUser** cmdlet. For details about using a sample script to assign **Line URI** to multiple user accounts, see [Assign Line URIs to Multiple Users](#).

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-UserAdministrator** or **CsAdministrator** role.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the search field, type the name of the user you want to configure for dial-in conferencing or click **Add filter** to specify search fields, and then click **Find**.
5. Double-click the user name to open the **Edit Skype for Business Server User** dialog box.
6. Under **Telephony**, in the **Line URI** field, type a unique, normalized phone number (for example, tel:+14255550200).

### NOTE

You can specify **Line URI** only if **Telephony** is set to **PC-to-PC only**, **Enterprise Voice**, **Remote call control** or **Remote call control only**.

7. Click **Commit**.

# Deploy SRS v1 Administrative Web Portal in Skype for Business Server

8/7/2019 • 8 minutes to read

The Skype for Business Server Skype Room Systems v1 (SRS v1, formerly known as Lync Room System) Administrative Web Portal is a web portal that organizations can use to maintain their Skype Room Systems conference rooms. Administrators can use the SRS v1 Administrative Web Portal to monitor device health, for example by monitoring audio/video devices. With this portal, administrators can remotely collect diagnostic information to monitor conference room health.

To use this feature, the SRS v1 Administrative Web Portal needs to be deployed on every Skype for Business Server Front End Server. This guide provides instructions for administrators on how to install and configure the SRS Administrative Web Portal. It is intended for administrators who have knowledge of Skype for Business Server administration, and who have administrator user rights to modify the Skype for Business Server topology.

After the SRS v1 Administrative Web Portal is deployed on the server, administrators can check the status SRS v1 devices by logging on to the site from their own computers or laptops.

## IMPORTANT

Download the [Microsoft Skype Room Systems v1 Administrative Web Portal for Skype for Business Server 2015](#).

In this topic:

- [Configure your environment for the SRS v1 Administrative Web Portal](#)
- [Install the SRS v1 Administrative Web Portal](#)
- [Use the SRS Administrative Web Portal](#)

## Configure your environment for the SRS v1 Administrative Web Portal

To use the SRS v1 Administrative Web Portal, you will need to install or configure the following prerequisites.

## IMPORTANT

If the server is configured with both Kerberos and NTLM authentication, and SRS is running on a computer that is not joined to the domain, Kerberos authentication will fail and the user will not see the status of SRS in the administrative portal. To resolve this issue, configure the server with NTLM authentication or both NTLM and TLS-DSK authentication (without Kerberos), or join the SRS computer to the domain.

1. Install Skype for Business Server Cumulative Updates in the Skype for Business Server topology.

To get the update or see what's included with it, see [Updates for Skype for Business Server 2015](#).

2. Create a SIP-enabled Active Directory user.

The SRS v1 Administrative Web Portal uses these credentials to query information from Skype for Business Server. The username in the examples given is LRSApp.

3. Create an Active Directory security group with name LRSSupportAdminGroup.

Create the group with Group Scope as Global and Group Type as Security. SIP enabled users who are added to this group will be authorized to see the list of rooms and execute certain commands, such as collecting logs.

4. Create an Active Directory security group with name LRSFullAccessAdminGroup.

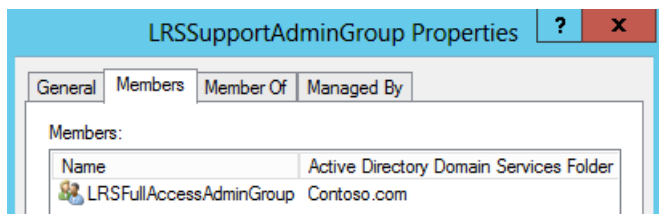
Create the group with Group Scope as Global and Group Type as Security. SIP enabled users who are added to this group are authorized to use all admin portal functionality on a single Skype room. To include support for bulk management of Skype rooms, refer to step 5.



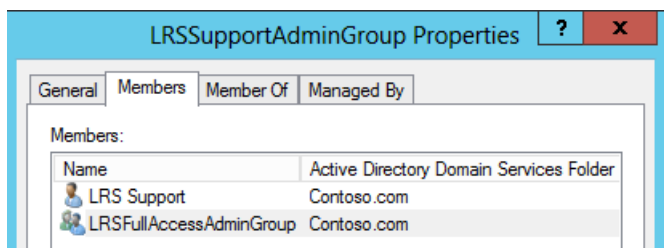
5. Create an Active Directory security group with name LRSPowerUserAdminsGroup.

Create the group with Group Scope as Global and Group Type as Security. SIP enabled users who are added to this group are authorized to use all admin portal functionality including bulk management of Skype for Business rooms.

6. Add LRSFullAccessAdminGroup as a member of LRSSupportAdminGroup.



7. Create a SIP enabled Active Directory user with name LRSSupport. Add this user to LRSSupportAdminGroup.



8. Install [ASP.NET MVC 4 for Visual Studio 2010 SP1 and Visual Web Developer 2010 SP1](#).

## Install the SRS v1 Administrative Web Portal

Download the [Microsoft Skype Room Systems v1 Administrative Web Portal for Skype for Business Server 2015](#).

To install the SRS v1 Administrative Web Portal, use the following steps.

1. Configure the Trusted Application Port by running the following cmdlet in Skype for Business Server Management Shell:

```
Set-CsWebServer -Identity POOLFQDN -MeetingRoomAdminPortalInternalListeningPort 4456 -  
MeetingRoomAdminPortalExternalListeningPort 4457
```

2. To install the Meeting Room Portal, download **MeetingRoomPortalInstaller.msi** and then run it as an administrator.

3. Open the Web.config file from the following location:

%Program Files%\Skype for Business Server 2015\Web Components\Meeting Room Portal\Int\Handler\

4. In the Web.Config file, change the PortalUserName to the username created in Step 2 under the section "[Configure your environment for the SRS v1 Administrative Web Portal](#)" (the recommended name in the step is LRSApp):

```
<add key="PortalUserName" value="sip:LRSApp@domain.com" />
```

5. Because the SRS v1 Admin Portal is a trusted application, you do not need to provide the password in the portal configuration. If this user is using a different registrar than local registrar, you need to specify the registrar for it by adding the following line in the Web.Config file:

```
<add key="PortalUserRegistrarFQDN" value="pool-xxxx.domain.com" />
```

6. If the port used is other than 5061, add the following line in the Web.Config file:

```
<add key="PortalUserRegistrarPort" value="5061" />
```

### Verify Installation of the SRS Administrative Web Portal


To verify installation of the SRS v1 Administrative Web Portal, do the following:

1. On a Front End server, browse to the following URL:

https://<fe-server>/lrs

You should not see any errors, as shown in the following image:

## Skype Room Systems Admin Portal

 Please sign in to continue.

### Sign In

User Name

Example: domain\username or username@domain.com

Password

Sign In

2. If you do not see any errors, try accessing the following URL from any other computer in the topology:

https://<fe-server>/lrs

To access the page, you will need to add the DNS records as described in "[Required DNS Records for Automatic Client Sign-In](#)."

## Use the SRS Administrative Web Portal

After you deploy SRS on the server, you can check the status of all SRS rooms by signing into the SRS v1 Administrative Web Portal from a browser.

### Sign in

1. Browse to the following URL:

https://<fe-server>/lrs

2. Enter the credentials for the LRSSupport account or an account that was added to the LRSSupportAdminGroup security group.

## Skype Room Systems Admin Portal

Please sign in to continue.

### Sign In

User Name

Example: domain\username or username@domain.com

Password

Sign In

### SRS Administrative Web Portal Summary Page

The summary page provides the following information for all of the SRS rooms deployed on the server:

- **Tag** The custom name that the administrator gives to the room. The Tag can be set in the portal by clicking on the room name.
- **Health** The health status of the room, which is derived from the Aggregate Health status of the room, which is shown under the Health section of the Room Settings page.
- **Next Meeting** The date and time the next meeting is scheduled.
- **SRS Version, Manufacturer, Model** These values are preset in SRS. Depending on the manufacturer, these fields might be left blank.
- **Last Refresh** Displays the last time the web page was refreshed.

#### Skype Room Systems Admin Portal

Room Name	Tag	Health	Status	Next Meeting	SRS Version	Auto update	Manufacturer	Model	Last Refresh
Conf Room JHB Shingwedzi LRS	0	Offline	Offline		15.13.1	Not enabled	SMART Technologies	SMART Room System	Jan 19, 2017 7:54 AM
Conf Room JHB Ibhusezi Skype Room	MSIT - CR JHB LRS Ibhusezi	Online	Away		15.15.0	Not enabled	SMART Technologies	SMART Room System	Jan 24, 2017 10:51 AM
Conf Rm - Skype TLL Korvits (10) LRS	LRS Tallinn	Offline	Offline		15.13.5	Not enabled	Crestron Electronics, Inc.	CCS-UC-CODEC-100	Dec 15, 2015 8:36 AM
Conf Rm Kista 00/Biblioteksgatan Skype Room	MSIT - Kista 00/Biblioteksgatan	Offline	Offline		15.14.9	Enabled	SMART Technologies	SMART Room System	Apr 01, 2016 4:49 AM
Espoo Test LRS	0	Offline	Offline		15.12.1	Not enabled	Crestron Electronics, Inc.	CCS-UC-CODEC-100	Nov 18, 2015 11:48 PM
Fabriek Skype Room	0	Offline	Offline		15.15.4	Enabled	SMART Technologies	SMART Room System	Aug 16, 2016 4:12 AM
Ltd 2KS LCC Twickenham (8) Skype Room	0	Online	Away		15.15.5	Not enabled	SMART Technologies	SMART Room System	Jan 24, 2017 10:51 AM
Conf Room MSRC-UK-0359-Mint (Bp) AV Roundtable	0	Offline	Offline		15.13.5	Not enabled	Crestron Electronics, Inc.	CCS-UC-CODEC-100	Aug 13, 2015 5:33 AM
Warsaw LRS	0	Offline	Offline		15.14.2	Not enabled	SMART Technologies	SMART Room System	Sep 26, 2016 12:28 AM
Conf Room Paris - C2503 - Seine9 (12) Skype Room	MSIT - Paris C2503 Seine9	Online	Away		15.14.9	Not enabled	Crestron Electronics, Inc.	CCS-UC-CODEC-100	Jan 24, 2017 10:51 AM
Conf Rm CIE Brussels Skype Room	0	Offline	Offline		15.15.5	Not enabled	SMART Technologies	SMART Room System	Dec 15, 2016 5:59 PM
Conf Room Berlin 4006 Mitte (10) Skype Room	0	Online	Away		15.14.9	Not enabled	SMART Technologies	SMART Room System	Jan 24, 2017 10:51 AM
Conf Room Milano 018 LRS	0	Offline	Offline		15.15.3	Not enabled	Crestron Electronics, Inc.	CCS-UC-CODEC-100	Jan 23, 2017 2:37 AM
EDI Watt Room Skype Room	MSIT - EDI Watt Room	Online	Away		15.15.5	Not enabled	SMART Technologies	SMART Room System	Jan 24, 2017 10:51 AM
Conf Room Kista 0/Vision (150) Skype Room	0	Online	Away		15.14.9	Not enabled	Crestron Electronics, Inc.	CCS-UC-CODEC-200	Jan 24, 2017 10:51 AM

#### NOTE

You will only see the Bulk Management menu if you are part of the LRSPowerUserAdminsGroup security group.

### SRS Room Information

The Room Info section of the portal allows you to view and configure individual SRS rooms. It contains four sections: Settings, Details, Logging, and Health.

## Settings

In the Settings section, you can set the password, room tag, and default volume levels for the room. If you configure these settings, the changes are replicated only after you restart the SRS console. You will only see System Updates settings for SRS devices using release 15.12 and later.

### [Skype Room Systems Admin Portal](#) > [Conf Room 113/3181\(20\) Skype Room](#)

**Room Info**

- Settings
- Details
- Troubleshooting
- Health

**Credentials**

Password

Show password

**Room Tag**

Tag

**System Updates**

Automatically update

**Audio**

Default Speaker Volume

Default Microphone Volume

Default Ringer Volume

## Details

The Details section provides a read-only summary of the SRS room's settings, including: the time of last refresh; next meeting; last updates, maintenance and calibration; default speaker, mic, and ringer settings; version; SIP URI; number of screens and details about each screen; status, and activity.

## [Skype Room Systems Admin Portal](#) > [Conf Room 113/3181\(20\) Skype Room](#)

Room Info	Room name:	Conf Room 113/3181(20) Skype Room
Settings	Tag:	0
Details	Last refresh:	Jan 24, 2017 11:11 AM
Troubleshooting	Next meeting:	
Health	Last check for updates:	Nov 14, 2016 3:00 AM
	Last maintenance:	Jan 24, 2017 3:00 AM
	Last calibration:	
	Default speaker volume:	40%
	Default mic volume:	40%
	Default ringer volume:	40%
	System mode:	Meeting
	Manufacturer:	Crestron Electronics, Inc.
	Model:	CCS-UC-CODEC-200
	Major version:	15
	Minor version:	15
	Hotfix version:	6
	SIP URI:	cfb3181@microsoft.com
	User name:	redmond\cfb3181
	Last software update:	
	Number of screens:	2
	Left screen info:	HDMI1
	Right screen info:	HDMI1
	Console screen info:	DM
	Speaker info:	Speakerphone (AV Bridge CONFERENCE)
	Mic info:	Speakerphone (AV Bridge CONFERENCE)
	Content capture card info:	
	Camera info:	
	PC info:	
	Status:	Away
	Activity:	







### Troubleshooting

The Troubleshooting section can be used to remotely collect logs and save them to a specified location. You can also restart the SRS console (SRS user interface) or restart the entire system. To collect logs, provide a folder path in the specified format and make sure that the folder has write permissions given to the SRS machine account. If the log size is too big, it can take up to 5 minutes to finish collecting logs. Refreshing the page will give you the latest status.

### Health

The Health section gives a visual indication of the health of the Skype for Business Server connection, audio device, video device, resiliency state, and screen device.

## [Skype Room Systems Admin Portal](#) > [Conf Room 113/3181\(20\) Skype Room](#)

Room Info	Health
Settings	Aggregate state 
Details	Skype Server connection 
Troubleshooting	Audio device 
Health	Video device 
	LRS resiliency state (BOR) 
	Screen device 



## Additional Notes about the Administrative Web Portal

### NOTE

Setting changes are applied only after the SRS system is restarted.> If the LRSApp account password expires, you will not be able to see the status of the rooms. Configure the LRSAppuser account password so that it never expires, or be sure to update the password when it is near expiration.> The SRS administrative web portal is supported for on-premises deployments only.

### Bulk management

Bulk management of SRS rooms is a feature designed for advanced IT administrators, to simplify their workflow, and enable them with a time-saving convenient tool to remotely manage multiple rooms in a bulk fashion.

In order to see this functionality, the user need to be provisioned as a member of the special security group, **LRSPowerUserAdminsGroup**.

There is no limit to the number of SRS rooms you can select for bulk management. However, you can perform only one bulk management operation at a time.

To perform a bulk management operation, select the rooms you want to monitor, and click on the Bulk management menu.

### Frequently asked questions

#### Why can't I sign in to the administrative web portal?

When you open <https://localhost/lrs>, you will be able to see the sign in page, but when you type in your credentials, you cannot sign in. In this case, you must open <https://FQDNofFeserver/SRS> to sign in to the administrative web portal.

#### Why can't I see SRS v1 in the administrative web portal?

- Make sure you have SRS accounts in your deployment and that they are created according to the SRS Administrative Web Portal deployment recommendations. Make sure the SRS accounts are provisioned using `Enable-CsMeetingRoom`, not `Enable-CsUser`, on the Skype for Business Server.
- If you have created SRS accounts and cannot see the accounts in administrative web portal, collect the server logs by using the Skype for Business Server Logging tool with the **MeetingPortal** component selected, and then send them to your SRS support contact.
- If you have created SRS accounts and cannot see the accounts in administrative web portal, collect the client logs using Fiddler, and also copy the console log from the browser development tools, and then send them to your SRS support contact. You can also modify the trace level value in the `Web.config` to get a more detailed log.

```
<system.diagnostics>
  <switches>
    <!--
      This switch controls logging message levels. 0 implies
      logging is turned off. 1 implies only errors are logged,
      2 implies errors & warnings. 4 is the most detailed.
    -->
    <add name="TraceLevelSwitch" value="3" />
  </switches>
</system.diagnostics>
```

#### Why can't I see the status of SRS in the administrative web portal?

- Make sure that the LRSApp user account is SIP-enabled.
- If you are still having issues, collect the **Trace.log** file in the SRS system from `D:\Tracing\LRAdminLogs`, and then send it to your SRS support contact.

**Why can't I see the bulk management menus for SRS in the administrative web portal?**

Make sure that the LRSApp user account is SIP-enabled, and is part of the LRSPowerUserAdminsGroup security group.

**Does the SRS v1 administrative web portal work with Microsoft Teams Rooms?**

No.

# Deploy Edge Server in Skype for Business Server

8/21/2019 • 2 minutes to read

**Summary:** Learn how to deploy an Edge Server or an Edge pool into your Skype for Business Server environment.

Why deploy an Edge Server or an Edge pool into your Skype for Business Server environment? It's necessary if you need external users who aren't logged into your organization's internal network to be able to interact with internal users. These external users could be authenticated and anonymous remote users, federated partners, or other mobile clients.

## Deployment checklist for the Edge, for Skype for Business Server

As noted above, a lot goes into an Edge Server deployment for Skype for Business Server. This checklist gives you an overview of the tasks you'll need to perform, and links to more detailed steps.

We hope you've begun in the [Plan for Edge Server deployments in Skype for Business Server](#) section. If not, many of the things we refer to are detailed there. The deployment section contains only procedures, so if you want to know the reasoning behind these steps, planning is the place to begin.

This documentation also presumes you've already completed the Basic Deployment of Skype for Business Server. You may be doing that deployment side-by-side with the Edge, but you do need to follow those steps first, and then you'll be able to make the topology changes for the Edge that are documented here.

These are the high-level steps you'll need to follow, and the places you'll find those steps:

- [Edge Server system requirements in Skype for Business Server](#)
- [Edge Server environmental requirements in Skype for Business Server](#)
- [Create your Edge topology for Skype for Business Server](#)
- [Deploy Edge Servers in Skype for Business Server](#)
- [Validate your Edge deployment in Skype for Business Server](#)

# Create your Edge topology for Skype for Business Server

8/7/2019 • 15 minutes to read

**Summary:** Learn how to build, publish, and export your Edge Server topology in Skype for Business Server.

Topology Builder is the tool you need to use to build your Edge Server topology, just as it's used for any topology component for Skype for Business Server. Before following the steps below, you will need to have set up at least one Front End pool or a Standard Edition server.

We cover the following topics in this article:

- Build your Edge Server topology
- Publish your Edge Server topology
- Export your Edge Server topology

## NOTE

To follow the steps below, you're going to need to log into the domain servers mentioned below as a user who's a member of the following domain groups:

- RTCUniversalServerAdmins
- Domain Admins

## Build your Edge Server topology

The first deployment step is building your Skype for Business Server Edge Server topology, which consists of one of three options:

- A single Edge Server
- A DNS load balanced Edge pool (one or more servers)
- A hardware load balanced Edge pool (one or more servers)

If you aren't sure what you need, then before you start following these steps, it's a good time to go over the Planning documentation. Otherwise, let's begin.

### Defining the topology for a single Edge Server

1. Log onto your Skype for Business Server Standard Edition server, or a Skype for Business Server Front End pool.
2. Once there, open **Skype for Business Server Topology Builder**.
3. In the console tree, expand the site you're going to deploy the Edge Server to.
4. Right-click **Edge pools**, and then click **New Edge pool**.
5. You'll click **Next** on the **Define New Edge pool** screen.
6. On the **Define the Edge pool FQDN** screen, type the internal fully qualified domain name (FQDN) that

the Edge Server is going to use, and select **Single computer pool**, clicking **Next** when done.

7. On the **Select features** screen, you have a choice:

- You may intend to use the same FQDN and IP address for your SIP Access service, your Skype for Business Server Web Conferencing service, and your A/V Edge service. If so, you need to choose the **Use a single FQDN and IP address checkbox** (and keep this in mind for Step 9 below)
- If you're planning to enable federation, choose the **Enable federation for this Edge pool (Port 5061)** check box.

8. Once you've clicked **Next**, you'll find yourself on the **IP Options** screen. Your options are as follows:

- Enable IPv4 on the internal interface
- Enable IPv6 on the internal interface
- Enable IPv4 on the external interface
- Enable IPv6 on the external interface

These are pretty self-explanatory, whether you're using IPv4 or IPv6 addresses, and you're applying those addresses on your Edge Server internally or externally (you'll need to keep this in mind for Step 10). You also have the option of configuring your Edge Server or your Edge pool to use a network address translation (NAT) address for the external IP address. You can do this by choosing **The external IP address of this Edge pool is translated by NAT** check box. Click **Next** when ready.

9. On the External FQDNs screen, your choices depend on the selection you made in Step 7 above.

- If you checked the **Use a single FQDN and IP Address** check box, you need to enter your single external FQDN in the **SIP Access** box. Then you'll need to enter different port numbers for each edge service to allow them all to connect independently. We recommend 5061 for the **SIP Access** Edge service, 444 for the **Web Conferencing** Edge service, and 443 for the **A/V** Edge service. Click **Next** when done.
- If you didn't check the **Use a single FQDN and IP Address** check box, you'll now need to enter the three external FQDNs for the **SIP Access** Edge service, the **Web Conferencing** Edge service, and the **A/V** Edge service. Click **Next** when done.

10. You're now on the **Define the Internal IP address** screen. Here you'll type the IP address of your Edge Server in the **Internal IPv4 address** and **Internal IPv6 address** text boxes, depending on the choices you made back in Step 8. Click **Next** when ready.

11. On the **Define the External IP address** screen, you have a few options depending on your previous choices:

- You may be using a single FQDN for all services. If so, type your external IPv4 or IPv6 address (whichever you're using) into the **SIP Access** text box, and then click **Next**.
- You may have chosen to use three separate FQDNs and IP addresses for the services. If that's the case, enter your external IPv4 or IPv6 addresses for the **SIP Access** Edge service, the **Web Conferencing** Edge service, and the **A/V** Edge service, and then click **Next**.

#### NOTE

If you didn't previously choose to enable and assign IPv6 addressing, you won't see this dialog box. That's normal, just go to the next step.

12. If you chose to use NAT back in Step 8, you'll now get a screen with a **Public IP address** textbox. You'll

need to enter the public IPv4 and/or IPv6 address you've set for the A/V Edge service, to be translated by NAT. Then click **Next**.

- Next screen up is **Define the next hop**. In the **Next hop pool** box, select the name of your internal pool, which might be a Front End pool or a Standalone pool. If you have a Director in your environment, you should choose the Director. Then click **Next**.
- On the **Associate Front End pools** screen, you'll need to specify one or more internal pools, including Front End pools and Standard Edition servers, to associate with this Edge Server. Just choose the names of the internal pools you want using this Edge Server to communicate with supported external users. Click **Next**.

#### NOTE

Something to keep in mind here is, if your internal pools or standalone servers are already using a different Skype for Business Server Edge Server, they can't have multiple associations. If you choose an internal pool or standalone server that's in that situation, you'll see a warning appear telling you about the other Edge Server, and you can decide whether you want to continue or not. If you go ahead with this new association, the connection to the other Edge Server will stop.

- Click **Finish** on the next screen.
- Now you'll be able to publish this updated technology, and follow the instructions in [Deploy Edge Servers in Skype for Business Server](#) to deploy to your Edge Server from here.

### Defining the topology for a DNS load balanced Edge Server pool

- Log onto your Skype for Business Server Standard Edition server, or a Skype for Business Server Front End Server.
- Once there, open **Skype for Business Server Topology Builder**.
- In the console tree, expand the site you're going to deploy the Edge Server to.
- Right-click **Edge pools**, and then click **New Edge pool**.
- You'll click **Next** on the **Define New Edge pool** screen.
- On the **Define the Edge pool FQDN** screen, type the internal fully qualified domain name (FQDN) that the Edge pool is going to use, and select **Multiple computer pool**, clicking **Next** when done.
- On the **Select features** screen, you have a choice:
  - You may intend to use the same FQDN and IP address for your SIP Access service, your Skype for Business Server Web Conferencing Service, and your A/V Edge service. If so, you need to choose the **Use a single FQDN and IP address checkbox** (and keep this in mind for Step 9 below)
  - If you're planning to enable federation, choose the **Enable federation for this Edge pool (Port 5061)** check box.
- Once you've clicked **Next**, you'll find yourself on the **IP Options** screen. Your options are as follows:
  - Enable IPv4 on the internal interface
  - Enable IPv6 on the internal interface
  - Enable IPv4 on the external interface
  - Enable IPv6 on the external interface

These are pretty self-explanatory, whether you're using IPv4 or IPv6 addresses, and you're applying

those addresses on your Edge Server internally or externally (you'll need to keep this in mind for Step 11). You also have the option of configuring your Edge Server or your Edge pool to use a network address translation (NAT) address for the external IP address. You can do this by choosing **The external IP address of this Edge pool is translated by NAT** check box . Click **Next** when ready.

9. On the External FQDNs screen, your choices depend on the selection you made in Step 7 above.
  - If you checked the **Use a single FQDN and IP Address** check box, you need to enter your single external FQDN in the **SIP Access** box. Then you'll need to enter different port numbers for each edge service to allow them all to connect independently. We recommend 5061 for the **SIP Access** Edge service, 444 for the **Web Conferencing** Edge service, and 443 for the **A/V** Edge service. Click **Next** when done.
  - If you didn't check the **Use a single FQDN and IP Address** check box, you'll now need to enter the three external FQDNs for the **SIP Access** Edge service, the **Web Conferencing** Edge service, and the **A/V** Edge service. Click **Next** when done.
10. Now you've reached the **Define the computers in this pool** screen. Click the **Add** button.
11. You're now on the **Define the Internal IP address** screen. Here you'll type the IP address of your Edge Server in the **Internal IPv4 address** and **Internal IPv6 address** text boxes, depending on the choices you made back in Step 8. Click **Next** when ready.
12. On the **Define the External IP address** screen, you have a few options depending on your previous choices:
  - You may be using a single FQDN for all services. If so, type your external IPv4 or IPv6 address (whichever you're using) into the **SIP Access** text box, and then click **Next**.
  - You may have chosen to use three separate FQDNs and IP addresses for the services. If that's the case, enter your external IPv4 or IPv6 addresses for the **SIP Access** Edge service, the **Web Conferencing** Edge service, and the **A/V** Edge service, and then click **Next**.

#### NOTE

If you didn't previously choose to enable and assign IPv6 addressing, you won't see this dialog box. That's normal, just go to the next step.

13. Click **Finish**. The Edge Server you just created should now be listed in the **Define the computers in this pool** dialog box.
14. While still on the **Define the computers in this pool** screen, click the **Add** button again and repeat steps 11 through 13 until you've added all the Edge Servers you intend to have in this pool. When this is complete, click **Next**.
15. If you chose to use NAT back in Step 8, you'll now get a screen with a **Public IP address** textbox. You'll need to enter the public IPv4 and/or IPv6 address you've set for the A/V Edge service, to be translated by NAT. Then click **Next**.
16. Next screen up is **Define the next hop**. In the **Next hop pool** box, select the name of your internal pool, which might be a Front End pool or a Standalone pool. If you have a Director in your environment, you should choose the Director. Then click **Next**.
17. On the **Associate Front End pools** screen, you'll need to specify one or more internal pools, including Front End pools and Standard Edition pools, to associate with this Edge Server. Just choose the names of the internal pools you want using this Edge Server to communicate with supported external users. Click

## Next.

### NOTE

Something to keep in mind here is, if your internal pools or standalone servers are already using a different Skype for Business Server Edge Server, they can't have multiple associations. If you choose an internal pool or standalone server that's in that situation, you'll see a warning appear telling you about the other Edge Server, and you can decide whether you want to continue or not. If you go ahead with this new association, the connection to the other Edge Server will stop.

18. Click **Finish** on the next screen.
19. Now you'll be able to publish this updated technology, and follow the instructions in [Deploy Edge Servers in Skype for Business Server](#) to deploy to your Edge Server from here.

### Defining the topology for a hardware load balanced Edge Server pool

1. Log onto your Skype for Business Server Standard Edition server, or a Skype for Business Server Front End Server.
2. Once there, open **Skype for Business Server Topology Builder**.
3. In the console tree, expand the site you're going to deploy the Edge Server to.
4. Right-click **Edge pools**, and then click **New Edge pool**.
5. You'll click **Next** on the **Define New Edge pool** screen.
6. On the **Define the Edge pool FQDN** screen, type the internal fully qualified domain name (FQDN) that the Edge pool is going to use, and select **Multiple computer pool**, clicking **Next** when done.
7. On the **Select features** screen, you have a choice:
  - You may intend to use the same FQDN and IP address for your SIP Access service, your Skype for Business Server Web Conferencing Service, and your A/V Edge service. If so, you need to choose the **Use a single FQDN and IP address checkbox** (and keep this in mind for Step 9 below)
  - If you're planning to enable federation, choose the **Enable federation for this Edge pool (Port 5061)** check box.
8. Once you've clicked **Next**, you'll find yourself on the **IP Options** screen. Your options are as follows:
  - Enable IPv4 on the internal interface
  - Enable IPv6 on the internal interface
  - Enable IPv4 on the external interface
  - Enable IPv6 on the external interface

These are pretty self-explanatory, whether you're using IPv4 or IPv6 addresses, and you're applying those addresses on your Edge Server internally or externally (you'll need to keep this in mind for Step 11).

### NOTE

Unlike the other two topology options, when using a hardware load balancer, you **MUST NOT** select the option **The external IP address of the Edge Pool is translated by NAT**. This is **not supported**.

9. On the External FQDNs screen, your choices depend on the selection you made in Step 7 above.



- If you checked the **Use a single FQDN and IP Address** check box, you need to enter your single external FQDN in the **SIP Access** box. Then you'll need to enter different port numbers for each edge service to allow them all to connect independently. We recommend 5061 for the **SIP Access** Edge service, 444 for the **Web Conferencing** Edge service, and 443 for the **A/V** Edge service. Click **Next** when done.
- If you didn't check the **Use a single FQDN and IP Address** check box, you'll now need to enter the three external FQDNs for the **SIP Access** Edge service, the **Web Conferencing** Edge service, and the **A/V** Edge service. Click **Next** when done.

10. Now you've reached the **Define the computers in this pool** screen. Click the **Add** button.
11. You're now on the **Define the Internal IP address** screen. Here you'll type the IP address of your Edge Server in the **Internal IPv4 address** and **Internal IPv6 address** text boxes, depending on the choices you made back in Step 8. Click **Next** when ready.
12. On the **Define the External IP address** screen, you have a few options depending on your previous choices:
  - You may be using a single FQDN for all services. If so, type your external IPv4 or IPv6 address (whichever you're using) into the **SIP Access** text box, and then click **Next**.
  - You may have chosen to use three separate FQDNs and IP addresses for the services. If that's the case, enter your external IPv4 or IPv6 addresses for the **SIP Access** Edge service, the **Web Conferencing** Edge service, and the **A/V** Edge service, and then click **Next**.

#### NOTE

If you didn't previously choose to enable and assign IPv6 addressing, you won't see this dialog box. That's normal, just go to the next step.

13. Click **Finish**. The Edge Server you just created should now be listed in the **Define the computers in this pool** dialog box.
14. While still on the **Define the computers in this pool** screen, click the **Add** button again and repeat steps 11 through 13 until you've added all the Edge Servers you intend to have in this pool. When this is complete, click **Next**.
15. Next screen up is **Define the next hop**. In the **Next hop pool** box, select the name of your internal pool, which might be a Front End pool or a Standalone pool. If you have a Director in your environment, you should choose the Director. Then click **Next**.
16. On the **Associate Front End pools** screen, you'll need to specify one or more internal pools, including Front End pools and Standard Edition pools, to associate with this Edge Server. Just choose the names of the internal pools you want using this Edge Server to communicate with supported external users. Click **Next**.

#### NOTE

Something to keep in mind here is, if your internal pools or standalone servers are already using a different Skype for Business Server Edge Server, they can't have multiple associations. If you choose an internal pool or standalone server that's in that situation, you'll see a warning appear telling you about the other Edge Server, and you can decide whether you want to continue or not. If you go ahead with this new association, the connection to the other Edge Server will stop.

17. Click **Finish** on the next screen.

18. Now you'll be able to publish this updated technology, and follow the instructions in [Deploy Edge Servers in Skype for Business Server](#) to deploy to your Edge Server from here.

## Publish your Edge Server topology

Once you've finished the steps above, it's time to publish this new topology, which will also allow you to export it to your Skype for Business Server Edge Server or Edge pool. Follow these steps:

1. Start **Topology Builder** (if it's not started already from the previous procedure).
2. In **Topology Builder**, in the console tree, right-click **Skype for Business Server** and then click **Skype for Business Server Topology Builder**.
3. On the **Welcome** page of the wizard, click **Next**.
4. On the **Create other databases** page, click **Next**.
5. When the status indicates that the database creation succeeded, do the following:
  - To view the log, click **View log**.
  - To close the wizard, click **Finish**.

## Export your Edge Server topology

To deploy successfully, the Skype for Business Server Deployment Wizard needs access to the Central Management store data. For internal servers in your domain or forest, this typically is straightforward. Edge Servers are outside of the domain, and so it's necessary to manually export the topology file to the Edge Server location, usually on a physical media. This export is done via PowerShell:

1. Start the **Skype for Business Server Management Shell**.
2. In the **Skype for Business Server Management Shell**, run the following:

```
Export-CsConfiguration -FileName <ConfigurationFilePath.zip>
```

3. Copy the exported file to external media (for example, a USB drive or network share that you can reach from the Edge Server's location).

# Deploy Edge Servers in Skype for Business Server

8/7/2019 • 20 minutes to read

**Summary:** Learn how to deploy Edge Servers into your Skype for Business Server environment.

The following sections contain steps that are meant to be followed after the Skype for Business Server [Plan for Edge Server deployments in Skype for Business Server](#) documentation has been reviewed. The deployment steps are as follows:

- Network interfaces
- Installation
- Certificates
- Starting the Edge Servers

## Network interfaces

As noted in Planning, you will either be configuring your network interface with DNS in the perimeter network hosting your Edge Servers, or without DNS in the perimeter network.

### Interface configuration with DNS servers in the perimeter network

1. Install two network adapters for each Edge Server, one for the internal-facing interface, and one for the external-facing interface.

#### NOTE

The internal and external subnets must not be routable to each other.

2. On your external interface, you'll configure **one** of the following:
  - a. Three static IP addresses on the external perimeter network subnet, and point the default gateway to the internal interface of the external firewall. Configure the adapter DNS settings to point to a pair of perimeter DNS servers.
  - b. One static IP address on the external perimeter network subnet, and point the default gateway to the internal interface of the external firewall. Configure the adapter DNS settings to point to a pair of perimeter DNS servers. This configuration is **ONLY** acceptable if you have previously configured your topology to have non-standard values in the port assignments, which is covered in the [Create your Edge topology for Skype for Business Server](#) article.
3. On your internal interface, configure one static IP on the internal perimeter network subnet, and don't set a default gateway. Configure the adaptor DNS settings to point to at least one DNS server, but preferably a pair of perimeter DNS servers.
4. Create persistent static routes on the internal interface to all internal networks where clients, Skype for Business Server, and Exchange Unified Messaging (UM) servers reside.

### Interface configuration without DNS servers in the perimeter network

1. Install two network adapters for each Edge Server, one for the internal-facing interface, and one for the external-facing interface.

#### NOTE

The internal and external subnets must not be routable to each other.

2. On your external interface, you'll configure **one** of the following:
  - a. Three static IP addresses on the external perimeter network subnet. You'll also need to configure the default gateway on the external interface, for example, defining the internet-facing router or the external firewall as the default gateway. Configure the adapter DNS settings to point to an external DNS server, ideally a pair of external DNS servers.
  - b. One static IP address on the external perimeter network subnet. You'll also need to configure the default gateway on the external interface, for example, defining the internet-facing router or the external firewall as the default gateway. Configure the adapter DNS settings to point to an external DNS server, or ideally a pair of external DNS servers. This configuration is **ONLY** acceptable if you have previously configured your topology to have non-standard values in the port assignments, which is covered in the [Create your Edge topology for Skype for Business Server](#) article.
3. On your internal interface, configure one static IP on the internal perimeter network subnet, and don't set a default gateway. Also leave the adapter DNS settings empty.
4. Create persistent static routes on the internal interface to all internal networks where clients, Skype for Business Server, and Exchange Unified Messaging (UM) servers reside.
5. Edit the HOST file on each Edge Server to contain a record for the next hop server or virtual IP (VIP). This record will be the Director, Standard Edition server or Front End pool you configured as the Edge Server next hop address in Topology Builder. If you're using DNS load balancing, include a line for each member of the next hop pool.

## Installation

To complete these steps successfully, you will need to have followed the steps in the [Create your Edge topology for Skype for Business Server](#) article.

1. Log onto the server you've been configuring for the Edge Server role with an account that's in the local Administrator's group.
2. You'll need the topology configuration file you copied out at the end of the Edge Server Topology documentation on this machine. Access the external media you placed that configuration file on (like a USB drive or share).
3. Start the **Deployment Wizard**.
4. Once the wizard opens, click **Install or Update Skype for Business Server System**.
5. The wizard will run checks to see if anything's already installed. As this is the first time running the wizard, you'll want to start at **Step 1. Install Local Configuration Store**.
6. The **Configure Local Replica of Central Management store** dialog will appear. You need to click **Import from a file (Recommended for Edge Servers)**.
7. From here, browse to the location of the topology you exported previously, select the .zip file, click **Open**, and then click **Next**.
8. The Deployment Wizard will read the configuration file and write the XML configuration file to the local computer.
9. After the **Executing Commands** process is finished, click **Finish**.

10. In the Deployment Wizard, click **Step 2. Setup or Remove Skype for Business Server Components**.

The wizard will then install the Skype for Business Server Edge components specified in the XML configuration file that's been stored on the local computer.

11. Once the installation's complete, you can move onto the steps in the **Certificates** section below.

## Certificates

The certificate requirements for the Edge Server can be found in the Edge Certificate Planning documentation.

The steps for setting up certificates are below.

### NOTE

When running the Certificate Wizard, you need to be logged in as an account with the correct permissions for the type of certificate template you're going to use. By default, a Skype for Business Server certificate request is going to use the Web Server certificate template. If you're logged in with an account that's a member of the RTCUniversalServerAdmins group to request a certificate via this template, double-check to make sure the group's been assigned the Enroll permissions to use that template.

### Internal Edge interface certificates

#### 1. Download or export the CA certification chain

##### a. Download using certsrv web site

i. Log into a Skype for Business Server in your internal network as a member of the local Administrators group.

ii. Open up **Start**, and **Run** (or **Search** and **Run** ), and then type the following:

```
https://<NAME OF YOUR ISSUING CA SERVER>/certsrv
```

For example:

```
https://ca01/contoso.com/certsrv
```

iii. On the issuing CA's certsrv web page, under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**.

iv. Under **Download a CA certificate, certificate chain, or CRL**, click **Download CA certificate chain**.

v. In the **File Download** box, click **Save**.

vi. Save the .p7b file to the hard disk drive on the server, and then copy it to a folder on each of your Edge Servers.

##### b. Export using MMC

i. You can export the CA root certificate from any domain joined machine using the MMC. Either go to **Start** and **Run**, or open **Search**, and type **MMC** to open.

ii. In the MMC console, click **File**, and then click **Add/Remove Snap-In**.

iii. From the **Add or Remove Snap-ins** dialog list, choose **Certificates**, and then click **Add**. When prompted, select **Computer Account**, and then **Next**. On the **Select Computer** dialog, select **Local Computer**. Click **Finish**, and then **OK**.

iv. Expand **Certificates (Local computer)**. Expand **Trusted Root Certification Authorities**. Select **Certificates**.

v. Click the root certificate issued by your CA. Right-click the certificate, choose **All Tasks** on the menu, and then select **Export**.

vi. The **Certificate Export Wizard** opens. Click **Next**.

vii. On the **Export File Format** dialog, choose the format you want to export to. Our recommendation is **Cryptographic Message Syntax Standard - PKCS #7 Certificates (P7b)**. If that's your choice as well, remember to also select the **Include all certificates in the certification path if possible** checkbox, as this will also export the certificate chain, including the root CA certificate and any Intermediate certificates. Click **Next**.

viii. On the **File to Export** dialog, in the file name entry, type a path and file name (the default extension would be .p7b) for the exported certificate. If it's easier on you, choose the **Browse** button to go to the location you want to save the exported certificate to, and name the exported certificate here. Click **Save**, and then **Next** when you're ready.

ix. Review the summary of your actions, and click **Finish** to complete the export of the certificate. Click **OK** to confirm the successful export.

x. Copy the .p7b file to each of your Edge Servers.

## 2. Import the CA certification chain

a. On each Edge Server, open the MMC (choose **Start** and **Run**, or **Search**, and type **MMC** to open).

b. On the **File** menu, click **Add/Remove Snap-in**, and then choose **Add**.

c. In the **Add or Remove Snap-ins** box, click **Certificates**, and then click **Add**.

d. In the **Certificate snap-in** dialog box, click **Computer account**, and then click **Next**.

e. In the **Select Computer** dialog box, ensure that the **Local Computer: (the computer this console is running on)** check box is selected, and then click **Finish**.

f. Click **Close**, and then **OK**.

g. In the console tree, expand **Certificates (Local Computer)**, right-click **Trusted Root Certification Authorities**, go to **All Tasks**, and then click **Import**.

h. In the wizard that appears, in the **File to Import** textbox, specify the file name of the certificate (the name you gave the .p7b file in the previous section). Click **Next**.

i. Leave the radio button on **Place all certificates in the following store, as Trusted Root Certification Authorities** should be selected. Click **Next**.

j. Review the summary, and click **Finish** to complete the import.

k. This will need to be done for every Edge Server you're deploying.

## 3. Create the certificate request

a. Log on to one of your Edge Servers, start the Deployment Wizard, and on **Step 3: Request, Install, or Assign Certificates**, click **Run** (or **Run Again**, if you've already run this wizard).

b. On the **Certificate Request** page, ensure **Internal Edge Certificate** is selected, and click **Request**.

c. On the **Delayed or Immediate Requests** page, choose **Send the request immediately to an online certification authority** if you have access to one from your Edge environment, or **Prepare the request now, but send it later** otherwise.

d. On the **Certificate Request File** page, enter the full part and file name for where the file will be saved (such as c:\SkypeInternalEdgeCert.cer). Click **Next**.

e. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer

template, check the **Use alternative certificate template for the selected Certificate Authority** check box. Otherwise, do nothing.

f. On the Name and Security Settings page, do the following:

i. In **Friendly name**, enter a display name for the certificate (such as Internal Edge).

ii. In **Bit length**, choose your bit length (the default is 2048, you can go higher and be more secure, but it will make performance slow down).

iii. If you need an exportable certificate, you must check the **Mark certificate private key as exportable** check box.

iv. Click **Next**.

g. On the **Organization Information** page, enter the name for your organization and organizational unit (OU). You might enter your division or department (IT, for example).

h. On the **Geographical Information** page, enter your location information.

i. On the **Subject Name/Subject Alternate Names** page, this should be auto-populated by the wizard.

j. On the **Configure Additional Subject Alternate Names** page, you need to add any additional subject alternative names that you need.

k. On the **Request Summary** page, look over the certificate information that's going to be used to generate your request. If you need to make changes, go back and do so now.

l. Then click **Next** to generate the CSR file you'll need to provide to the CA (you can also click **View Log** to look at the log for the certificate request).

m. Once the request has been generated, you can click **View** to look at the certificate, and **Finish** to close out the window. The contents of the CSR file need to be given to your CA, so they can generate a certificate for you to import to this computer in the next section.

#### 4. Import the certificate

a. Log on, as a member of the local Administrators group, to the Edge Server you made your certificate request from in the last procedure.

b. In the Deployment Wizard, next to **Step 3. Request, Install or Assign Certificates**, click **Run Again**.

c. On the **Available Certificates Tasks** page, click **Import a certificate from a .P7b, .pfx or .cer file**.

d. On the **Import Certificate** page, type the full path and file name of the certificate you got in the previous section (or you can click **Browse** to find and choose the file that way).

e. If you're importing certificates for other members of your Edge pool, and your certificate contains a private key, be sure to select the **Certificate file that contains certificate's private key** check box, and specify the password. Click **Next** to continue.

f. On the **Summary** page, click **Next** once you've confirmed the information, and **Finish** once the certificate is successfully imported.

#### 5. Export the certificate

a. Make sure you've logged onto the Edge Server you imported the certificate to previously, as a member of the local Administrators group.

b. Click **Start, Run** (or open **Search**), and type **MMC**.

c. From the MMC console, click **File**, and click **Add/Remove Snap-in**.

- d. From the **Add or Remove Snap-ins** box, click **Certificates**, and click **Add**.
- e. In the **Certificates** snap-in dialog box, choose **Computer account**. Click **Next**.
- f. On the **Select Computer** dialog, select **Local computer: (the computer this console is running on)**. Click **Finish**. Click **OK**, and the configuration of the MMC console is completed.
- g. Double-click **Certificates (Local Computer)** to expand the certificate stores. Double-click **Personal**, and then click **Certificates**.

#### NOTE

You may be here, and you don't see any certificates in the Certificates Personal store for the local computer. You don't need to hunt around, if the key's not there, the imported certificate didn't have a private key associated with it. Try the request and import steps above one more time, and if you're sure you got all that right, talk to your CA administrator or provider.

- h. In the **Certificates Personal store** for the local computer, right-click the certificate that you're exporting. Select **All Tasks** from the resulting menu, and then click **Export**.
- i. In the **Certificate Export Wizard**, click **Next**. Select **Yes, export the private key**. Click **Next**.
- j. On the **Export File Formats** dialog, select **Personal Information Exchange - PKCS#12 (.PFX)**, and then select the following:
  - i. Include all certificates in the certification path, if possible.
  - ii. Export all extended properties.

#### NOTE

**NEVER** select **Delete the private key if the export is successful**. It'll mean you have to reimport the certificate and private key back to this Edge Server.

- k. If you want to assign a password to protect the private key, you can type a password for the private key. Reenter the password to confirm, and then click **Next**.
- l. Type a path and file name for the exported certificate, using a file extension of **.pfx**. The path either needs to be accessible by the other Edge Servers in the pool, or you'll need to move the file by means of external media (such as a USB drive). Click **Next** when you've made your choice.
- m. Review the summary on the **Completing the Certificate Export Wizard** dialog, and then click **Finish**.
- n. Click **OK** in the successful export dialog.

## 6. Assign the certificate

- a. On EACH Edge Server, in the Deployment Wizard, next to **Step 3. Request, Install or Assign Certificates**, click **Run again**.
- b. On the **Available Certificates Tasks** page, click **Assign an existing certificate**.
- c. On the **Certificate Assignment** page, select **Edge Internal** in the list.
- d. On the **Certificate Store** page, select the certificate you've imported for the internal Edge (from the previous section).
- e. On the **Certificate Assignment Summary** page, look over the settings, and then click **Next** to assign the certificate.
- f. On the wizard completion page, click **Finish**.



g. Once you've completed this procedure, it's a really good idea to open the Certificates MMC snap-in on each Edge Server, expand **Certificates (Local computer)**, expand **Personal**, click **Certificates**, and confirm that the internal Edge certificate is listed in the details pane.

## External Edge interface certificates

### 1. Create the certificate request

a. Log on to one of your Edge Servers, start the Deployment Wizard, and on **Step 3: Request, Install, or Assign Certificates**, click **Run** (or **Run Again**, if you've already run this wizard).

b. On the **Available Certificate Tasks** page, click **Create a new certificate request**.

c. On the **Certificate Request** page, ensure **External Edge Certificate** is selected, and click **Next**.

d. On the **Delayed or Immediate Requests** page, click **Prepare the request now, but send it later**.

e. On the **Certificate Request File** page, enter the full part and file name for where the file will be saved (such as c:\SkypeInternalEdgeCert.cer). Click **Next**.

f. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer template, check the **Use alternative certificate template for the selected Certificate Authority** check box.

g. On the Name and Security Settings page, do the following:

i. In **Friendly name**, enter a display name for the certificate (such as External Edge).

ii. In **Bit length**, choose your bit length (the default is 2048, you can go higher and be more secure, but it will make performance slow down).

iii. If you need an exportable certificate, you must check the **Mark certificate private key as exportable** check box.

iv. Click **Next**.

h. On the **Organization Information** page, enter the name for your organization and organizational unit (OU). You might enter your division or department (IT, for example).

i. On the **Geographical Information** page, enter your location information.

j. On the **Subject Name/Subject Alternate Names** page, the needed information should be auto-populated by the wizard.

k. On the **SIP Domain Setting on Subject Alternate Names (SANs)** page, check the domain checkbox to add a sip. entry to the subject alternative names list.

l. On the **Configure Additional Subject Alternate Names** page, you need to add any additional subject alternative names that you need.

m. On the **Request Summary** page, look over the certificate information that's going to be used to generate your request. If you need to make changes, go back and do so now.

n. When you're ready, click **Next** to generate the CSR file you'll need to provide to the CA (you can also click **View Log** to look at the log for the certificate request).

o. Once the request has been generated, you can click **View** to look at the certificate, and **Finish** to close out the window. The contents of the CSR file need to be given to your CA, so they can generate a certificate for you to import to this computer in the next section.

p. (OPTIONAL) You may, when submitting the contents of the CSR, be asked for certain information, as follows (CAs vary greatly, so this may not be required):

- **Microsoft** as the server platform

- **IIS** as the version
- **Web Server** as the usage type
- **PKCS7** as the response format

## 2. Import the certificate

a. Log on, as a member of the local Administrators group, to the Edge Server you made your certificate request from in the last procedure.

b. In the Deployment Wizard, next to **Step 3. Request, Install or Assign Certificates**, click **Run Again**.

c. On the **Available Certificates Tasks** page, click **Import a certificate from a .P7b, .pfx or .cer file**.

d. On the **Import Certificate** page, type the full path and file name of the certificate you got in the previous section (or you can click **Browse** to find and choose the file that way). If your certificate contains a private key, make sure to select **Certificate file contains certificate's private key**, and enter the password for the private key. Click **Next** when ready.

e. On the **Import Certificate Summary** page, review the summary information, and click **Next**.

f. On the **Executing Commands** page, you can review the result of the import when it's complete by clicking **View Log**. Click **Finish** to complete the certificate import.

g. If you have other Edge Servers in a pool, you'll need to follow the next two procedures as well. If this is a standalone Edge Server, you're done with external certificates.

## 3. Export the certificate

a. Make sure you've logged onto the Edge Server you imported the certificate to as a local Administrator.

b. Click **Start, Run** (or open **Search** ), and type **MMC**.

c. From the MMC console, click **File**, and then click **Add/Remove Snap-in**.

d. From the **Add or Remove Snap-ins** box, click **Certificates**, and click **Add**.

e. In the **Certificates** snap-in dialog box, choose **Computer account**. Click **Next**.

f. On the **Select Computer** dialog, select **Local computer: (the computer this console is running on)**. Click **Finish**. Click **OK**, and the configuration of the MMC console is completed.

g. Double-click **Certificates (Local Computer)** to expand the certificate stores. **Double-click Personal**, and then click **Certificates**.

### NOTE

You may be here, and you don't see any certificates in the Certificates Personal store for the local computer. You don't need to hunt around, if the key's not there, the imported certificate didn't have a private key associated with it. Try the request and import steps above one more time, and if you're sure you got all that right, talk to your CA administrator or provider.

h. In the **Certificates Personal store** for the local computer, right-click the certificate that you're exporting. **Select All Tasks** from the resulting menu, and then click **Export**.

i. In the **Certificate Export Wizard**, click **Next**. Select **Yes, export the private key**. Click **Next**.

#### NOTE

If **Yes, export the private key** isn't available, then the private key for this certificate wasn't marked for export before you got it. You need to request the certificate from the provider again, with the private key set to export, before doing this successfully.

j. On the Export File Formats dialog, select Personal Information Exchange - PKCS#12 (.PFX) and then select the following:

- i. Include all certificates in the certification path, if possible.
- ii. Export all extended properties.

#### NOTE

**NEVER** select **Delete the private key if the export is successful**. It'll mean you have to reimport the certificate and private key back to this Edge Server.

k. If you want to assign a password to protect the private key, you can type a password for the private key. Reenter the password to confirm, and then click **Next**.

l. Type a path and file name for the exported certificate, using a file extension of **.pfx**. The path either needs to be accessible by the other Edge Servers in the pool, or you'll need to move the file by means of external media (such as a USB drive). Click **Next** when you've made your choice.

m. Review the summary on the **Completing the Certificate Export Wizard** dialog, and then click **Finish**.

n. Click **OK** in the successful export dialog.

o. You'll now need to go back to the Import the certificate section prior to this and import the certificate to all your remaining Edge Servers, then proceed with assigning, below.

#### 4. Assign the certificate

a. On **EACH** Edge Server, in the Deployment Wizard, next to **Step 3. Request, Install or Assign Certificates**, click **Run again**.

b. On the **Available Certificates Tasks** page, click **Assign an existing certificate**.

c. On the **Certificate Assignment** page, select **Edge External** in the list.

d. On the **Certificate Store** page, select the certificate you've imported for the external Edge (from the previous section).

e. On the **Certificate Assignment Summary** page, look over the settings, and then click **Next** to assign the certificate.

f. On the wizard completion page, click **Finish**.

g. Once you've completed this procedure, it's a really good idea to open the Certificates MMC snap-in on each server, expand **Certificates (Local computer)**, expand **Personal**, click **Certificates**, and confirm that the internal Edge certificate is listed in the details pane.

#### NOTE

You will also have needed to set up the certificates for your reverse proxy server.

## Starting the Edge Servers

Once the setup is complete, you'll need to start the services on each Edge server in your deployment:

1. On each Edge Server, in the **Deployment Wizard**, next to **Step 4: Start Services**, click **Run**.
2. On the **Start Skype for Business Server Services** page, review the list of services, and then click **Next** to start the services.
3. After the services are started, you can click **Finish** to close the wizard.
4. (Optional) Still under **Step 4: Start Services**, click **Services Status**.
5. In the **Services MMC** on each server, verify that all the Skype for Business Server services are running.

# Validate your Edge deployment in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn how to verify that your deployment of Edge Server or Edge Server pool is working in Skype for Business Server.

Once you've deployed your Edge Server or Edge Server pool, you need to know if it's working properly. Here are a couple of things that can help with confirming your Edge environment is connected to your internal servers, and also that your external users can connect to your Skype for Business Server environment through your Edge.

## Verify connectivity between your internal servers and your Edge servers

While validation of connectivity is done automatically in Edge Server or Edge Server pool when the Edge Servers are installed, you can still confirm this for yourself with Windows PowerShell. Run the `Get-CsManagementStoreReplicationStatus` cmdlet on the internal server which has the Central Management store, or any domain joined computer on which Skype for Business Server Core Components (OcsCore.msi) are installed.

The initial result of running this command may give a False status, rather than True, for replication. If that happens run the `Invoke-CsManagementStoreReplication` cmdlet. Give it some time to complete the replication, and then run the `Get-CsManagementStoreReplicationStatus` cmdlet again.

## Verify connectivity for your external users

We do have a great tool for confirming your Edge Server configuration, and the ability to connect, send and receive the correct messages for Edge Server scenarios. It's the [Remote Connectivity Analyzer site](#). This is a site that's managed and maintained by Microsoft Support. To use this tool, browse to the website and follow the instructions to choose the right scenario for you.

### Things to consider when testing external user connectivity

Any test for external user access needs to include each type of internal user your organization supports, which could include any or all of the following:

- Users from at least one federated domain (we do recommend testing them all though).
- Anonymous users.
- Users in your organization who are logged into Skype for Business remotely, but aren't using VPN.

These tests will determine whether your Edge Server is:

- Listening on the necessary ports by using a telnet client from outside your network.
  - For example: `telnet sip.contoso.com 443`
  - You should perform the preceding test on the ports you're using on your Edge Server or Edge Server pool, depending on your deployment.
- Performing accurate external DNS resolution.
  - From outside your network, ping each of the external FQDNs of your Edge Server or Edge Server pool. Even if the ping fails, you'll see the IP addresses, which you can compare the IP addresses you've previously assigned.



# Deploy and Configure Mobility for Skype for Business Server

8/7/2019 • 27 minutes to read

This article will walk you through the steps to configure an existing Skype for Business Server installation to use the Mobility service, allowing your mobile devices to be able to take advantage of Skype for Business Server Mobility features.

Having reviewed the [Plan for Mobility for Skype for Business Server](#) article, you should be ready to proceed with the steps below to deploy Mobility into your Skype for Business Server environment. The steps are as follows (and we're including in this table a permissions list):

PHASE	PERMISSIONS
<a href="#">Create DNS records</a>	Domain Admins DNSAdmins
<a href="#">Modify certificates</a>	Local Administrator
<a href="#">Configure the reverse proxy</a>	Local Administrator
<a href="#">Configure Autodiscover for Mobility with hybrid deployments</a>	Domain Admins
<a href="#">Test your Mobility deployment</a>	CsAdministrator
<a href="#">Configure for push notifications</a>	RtcUniversalServerAdmins
<a href="#">Configure Mobility policy</a>	CsAdministrator

All the following sections contain steps that assume you've read the Planning topic. If anything's confusing you, feel free to check out the information there.

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## Create DNS records

You may already have these as part of your Skype for Business Server environment, but you do need to create the following records for Autodiscovery to work:

- An internal DNS record to support mobile users who're connecting from within your organization's network.
- An external (or public) DNS record to support mobile users who're connecting from outside your organization's network.

These records can be either A (host) names or CNAME records (you don't have to make both, we're just including

the steps for everything here).

### Create an internal DNS CNAME record

1. Log into a DNS server in your network that's either a member of the **Domain Admins** group or the **DnsAdmins** group.
2. Click **Start**, Choose **Administrative Tools** (you may need to **Search** for it if it's not an option off the Start menu), and then click **DNS** to open the DNS administrative snap-in.
3. In the left-hand pane of the console window, you'll need to go to the domain that's home to your Skype for Business Server's Front End Servers, and expand the **Forward Lookup Zones** there.
4. Take a moment to see which of the following you have:
  - Any host A or AAAA records for your Front End Server (Standard or Enterprise) or Front End pool(s).
  - Any host A or AAAA records for a Director or Director pool (an optional configuration you may have in your deployment).
5. Once you've noted this, right-click your SIP domain name, and then choose **New Alias (CNAME)** from the menu.
6. In the **Alias name** textbox, type `lyncdiscoverinternal` for your host name, for the internal Autodiscover service URL.
7. In the **Fully qualified domain name (FQDN for target host)**, you'll need to type or browse to the internal Web Services FQDN for your Front End pool (or single Front End Server, or Director pool or Director), identified in step 4 above. Click OK when this is entered.
8. You'll need to create a new Autodiscover CNAME record in the forward lookup zone for each SIP domain supported in your Skype for Business Server environment.

### Create an external DNS CNAME record

1. These steps are generic, because we can't tell what public DNS provider you might be using, but we still want to help you out. Please log into your public DNS provider with an account that will be able to make new DNS records there.
2. At this point in time, a SIP domain should already exist there for Skype for Business Server. Expand the **Forward Lookup Zone** for this SIP domain, or otherwise open it up.
3. Take a moment to see which of the following you have:
  - Any host A or AAAA records for your Front End Server (Standard or Enterprise) or Front End pool(s).
  - Any host A or AAAA records for a Director or Director pool (an optional configuration you may have in your deployment).
4. Once you have that information, you should be able to select an option for creating a **New Alias (CNAME)**.
5. Now you should be able to enter an **Alias Name**, you need to enter `lyncdiscover` here for the external Autodiscover service URL.
6. Next there should be an area to enter in a **FQDN for target host**, this will need to be the FQDN for your Front End pool (or single Front End Server, or Director pool or Director), identified in step 3 above.
7. You may need to save here, or if you need to create additional CNAME records in the forward lookup zone of each SIP domain in your Skype for Business Server environment, you should do that, but once you're ready, save your work.

### Create an internal DNS A record



1. Log into a DNS server in your network that's either a member of the **Domain Admins** group or the **DnsAdmins** group.
2. Click **Start**, Choose **Administrative Tools** (you may need to **Search** for it if it's not an option off the Start menu), and then click **DNS** to open the DNS administrative snap-in.
3. In the left-hand pane of the console window, you'll need to go to the domain that's home to your Skype for Business Server's Front End Servers, and expand the **Forward Lookup Zones** there.
4. Take a moment to see which of the following you have:
  - Any host A or AAAA records for your Front End Server (Standard or Enterprise) or Front End pool(s).
  - Any host A or AAAA records for a Director or Director pool (an optional configuration you may have in your deployment).
5. Once you've noted this, right-click your SIP domain name, and then choose **New Host (A or AAAA)** from the menu.
6. In the **Name** textbox, type lyncdiscoverinternal for your host name, for the internal Autodiscover service URL.
7. In the **IP Address** textbox, type the internal Web Services IP address for your Front End pool (or single Front End Server, or Director pool or Director), identified in step 4 above.
8. When this is done, click **Add Host**, and then click **OK**.
9. You'll need to create a new Autodiscover A or AAAA records in the forward lookup zone for each SIP domain supported in your Skype for Business Server environment. To do this, repeat steps 6-8 as many times as needed.
10. When you're done, click **Done**.

#### **Create an external DNS A record**

1. These steps are generic, because we can't tell what public DNS provider you might be using, but we still want to help you out. Please log into your public DNS provider with an account that will be able to make new DNS records there.
2. At this point in time, a SIP domain should already exist there for Skype for Business Server. Expand the **Forward Lookup Zone** for this SIP domain, or otherwise open it up.
3. Take a moment to see which of the following you have:
  - Any host A or AAAA records for your Front End Server (Standard or Enterprise) or Front End pool(s).
  - Any host A or AAAA records for a Director or Director pool (an optional configuration you may have in your deployment).
4. Once you have that information, you should be able to select an option for creating a **New Host A or AAAA**.
5. Now you should be able to enter a **Name**, you need to enter lyncdiscover here for the external Autodiscover service URL.
6. Next there should be an area to enter in a **IP Address**, this will need to be the IP for your Front End pool (or single Front End Server, or Director pool or Director), identified in step 3 above.
7. You may need to save here, or if you need to create additional A or AAAA records in the forward lookup zone of each SIP domain for your Skype for Business Server environment, you should do that, but once you're ready, save your work.

# Modify certificates

If you have questions about Planning around certificates, we've documented that in our [Plan for Mobility for Skype for Business Server](#) article. Once you've reviewed that, we'll walk you through the following:

- Do I need new certificates?
- Requesting new certificates from your Certificate Authority (CA).
- Updating your in-place certificates with the replacements using PowerShell.
- Checking the certificates using the Certificates snapin in the Microsoft Management Console (MMC).

## Do I need new certificates?

1. First, you may need to check and see what certificates are in-place, and whether or not they have the entries you need. To do that, you'll need to log into your Skype for Business Server with an account that's a local Administrator. This account may also need to have rights to the issuing Certificate Authority (CA), for some of these steps.
2. Open the Skype for Business Server Management Shell (you can use Search to find it if you don't have it pinned to your Start menu or task bar).
3. It's going to be essential for you to know what certificates have been assigned before you try adding an updated certificate. So at the command, type:

```
Get-CsCertificate
```

4. The information from Step 3 will be unique to you. You need to look it over to determine if you have a single certificate that's been assigned for multiple things, or whether you have a different certificate assigned for the different components that need them. The **Use** parameter will tell you how a certificate's being used, and the **Thumbprint** parameter will tell you if it's all the same certificate, or multiple certs.
5. If you have the SAN entries recommended in our Planning section, you're good. If not, you'll need to request a new certificate, or multiple certificates (depending on your configuration) from your Certificate Authority.

## Request a new certificate, or certificates, from your Certificate Authority (CA)

1. After you've checked to see what SAN entries you have, you know you have a **single certificate** (after checking via the steps above), and you learned you don't have all the entries you need. A new certificate request needs to be made to your CA. Open your Skype for Business Server PowerShell:

- For a missing Autodiscover Service SAN (replacing the -Ca parameter with your own Certificate Authority path):

```
Request-CsCertificate -New -Type Default,WebServicesInternal,WebServicesExternal -Ca dc\myca -AllSipDomain -verbose
```

- Now, if you have multiple SIP domains, you can't use the AllSipDomain parameter as in the example above. You'll need to use the DomainName parameter instead. And when you use the DomainName parameter, you've got to define the FQDN for the lyncdiscoverinternal and lyncdiscover records. An example would be (replacing the -Ca parameter with your own Certificate Authority path):

```
Request-CsCertificate -New -Type Default,WebServicesInternal,WebServicesExternal -Ca dc\myca -DomainName "LyncdiscoverInternal.contoso.com, LyncdiscoverInternal.contoso.net" -verbose
```

2. Or, after you've checked to see what SAN entries you have, you found you have **multiple certificates** that

don't have all the entries you need. A new certificate request needs to be made to your CA. Open your Skype for Business Server PowerShell:

- For a missing Autodiscover Service SAN (replacing the -Ca parameter with your own Certificate Authority path):

```
Request-CsCertificate -New -Type WebServicesInternal -Ca dc\myca -AllSipDomain -verbose
```

- Now, if you have multiple SIP domains, you can't use the AllSipDomain parameter as in the example above. You'll need to use the DomainName parameter instead. And when you use the DomainName parameter, you've got to define the FQDN for the lyncdiscoverinternal and lyncdiscover records. Examples would be (replacing the -Ca parameter with your own Certificate Authority path):

```
Request-CsCertificate -New -Type WebServicesInternal -Ca dc\myca -DomainName  
"LyncdiscoverInternal.contoso.com, LyncdiscoverInternal.contoso.net" -verbose
```

```
Request-CsCertificate -New -Type WebServicesExternal -Ca dc\myca -DomainName "Lyncdiscover.contoso.com,  
Lyncdiscover.contoso.net" -verbose
```

- Once the new certificates have been generated by the CA, you're going to need to assign them.

### Assign certificates using Skype for Business Server Management Shell

- Depending on what you found in the Do I need new certifications section above, you need to run **one** of the following.
  - If you have a single certificate for everything (the thumbprints are identical) then you need to run this:

```
Set-CsCertificate -Type <certificate(s) from the Use parameter> -Thumbprint <unique identifier>
```

- If you've got different certificates for things (the thumbprints are all different), run this instead:

```
Set-CsCertificate -Type Default -Thumbprint <certificate thumbprint>  
Set-CsCertificate -Type WebServicesInternal -Thumbprint <certificate thumbprint>  
Set-CsCertificate -Type WebServicesExternal -Thumbprint <certificate thumbprint>
```

### Viewing certificates in the Microsoft Management Console (MMC)

1. You have an option to look at your certificates using the Certificates snap-in for the MMC. Simply type MMC into search and it should pop up as an application option,.
2. To add the Certificates snap-in, you'll need to click **File**, and then **Add/Remove Snap-In...** (or keyboard shortcut **Ctrl+M** would also work). **Certificates** will be an option in the left-hand pane, select it and then **Computer Account** in the pop-up window, then **Next**.
3. Still in the pop-up window, in all likelihood you're doing this on the computer that's home to the certificates you need to look at, so leave the selection on **Local Computer** if that's so. If you're working on a remote machine, change the radio button to **Another Computer** and then either enter that computer's FQDN or use the **Browse** button to search for that computer through AD. After selecting the computer, you'll need to click **Finish** when ready, and then **OK** to add the snap-in to the MMC.
4. Expand the **Certificates** section in the MMC's left-hand pane. Expand the **Personal** folder as well, and then select **Certificates**. This lets you see the certificates in this store.
5. You need to locate the certificate you want to view, right-click on it, and choose **Open**.

#### NOTE

How do you know what certificate this is? It should be either the single certificate assigned to everything for your farm, or you may have multiple certificates for different things, like Default, Internal Web Services, etc., in which case you may need to look at multiple certificates. Multiple certificates will have the same thumbprint.

6. Once you've gotten to the **Certificate** view, choose **Details**. This will let you see the certificate subject name when you select **Subject**, and the assigned subject name and associated properties are shown.
7. You'll also need to check the **Subject Alternate Name** entries. You'll find one or more of the following:
  - The pool name for this pool, or the single server name if this isn't a pool.
  - The server name that the certificate is assigned to.
  - Simple URL records, typically meet and dialin.
  - Web Services internal and Web Services external names (for example, webpool01.contoso.net, webpool01.contoso.com), based on choices made in Topology Builder and over-ridden Web Services selections.
  - If already assigned, the lyncdiscover.<sipdomain> and lyncdiscoverinternal.<sipdomain> records.  
You'll need to check multiple certificates if you have more than one assigned (check the Note above).
8. So, if you find lyncdiscover.<sipdomain> and lyncdiscoverinternal.<sipdomain> records, you've got this configured already. You can close the MMC.
9. If they aren't assigned, you'll either need to make a new certificate request (outlined above) or you need to install them post-request (we recommend the following the PowerShell above for that).

## Configure the reverse proxy

The steps below are not meant to be followed exactly. That's because in previous versions of the product, we'd have walked you through, for example, configuring Threat Management Gateway (TMG) and if you weren't using that, you'd need to work out your own version from there.

TMG is no longer being offered by Microsoft as a product, and if you still need to configure it, you can look at the [Lync Server 2013 steps](#). But the following information's intended to be more generally helpful, even if there's no way we can provide specific walkthrough steps for every Reverse proxy out there.

We have two main things to consider:

- Are you going to be doing your initial Autodiscover request over HTTPS (which we recommend)?
  - If you have a web publishing rule, you need to modify it.
  - If you don't have a web publishing rule yet, you need to create it.
- If you're doing your initial Autodiscover request over HTTP, then you'll need to create or modify that rule as well.

## NOTE

**Important** A Proxy time-out value is a number that will vary from deployment to deployment. You should monitor your deployment and modify the value for the best experience for clients. You may be able to set the value as low as 200. If you are supporting Lync mobile clients in your environment, you should set the value to 960 to allow for push notification time-outs from Office 365, which have a time-out value of 900. It is very likely that you will have to increase the time-out value to avoid client disconnects when the value is too low, or decrease the number if connections through the proxy do not disconnect but clear long after the client has disconnected. Monitoring and baselining what is usual for your environment is the only accurate way to determine the appropriate setting for this value.

### Modify the existing web publishing rule for your external Autodiscover SAN and URL

1. Open your Reverse proxy interface.
2. You'll need to locate your web publishing rule, and choose the Edit option (it may be on a menu or tab, depending on your Reverse proxy configuration).
3. There should be an area that states what this web publishing rule is applied to. You need to modify this rule for incoming sites or requests for sites. You're going to **add** a new entry.
4. Type the name of your Autodiscover site (the example we'll use is `lyncdiscover.contoso.com`), and click **OK** or **Save**, depending on your Reverse proxy's format.
5. You may have a new certificate that has the Autodiscover SAN entry in it. That needs to be installed as well and configured for use according to your Reverse proxy's settings. Be sure to save everything when the configuration is completed.
6. If your Reverse proxy has a **Test** functionality, then please make use of it, to ensure everything's working properly.
7. Now, you may need to repeat these steps if you have a Director or Director pool in your environment (this would mean you have a second rule).

### Create a web publishing rule for the external Autodiscover URL

1. Open your Reverse proxy interface.
2. You'll need to locate where in the interface you create your web publishing rules, and choose the **New** or **Create** option (it may be on a menu or tab, depending on your Reverse proxy configuration). You are looking for the option to create a new web publishing rule.
3. Typically, you will need to enter the following information:
  - **Name:** the name for your rule
  - **Rule Action:** In this case it's an **Allow** rule, you're letting something pass through your Reverse proxy.
  - The **Publishing** rule or option you're choosing would be **single web site or load balancer**.
  - This needs to be **SSL** for external access, choose that option.
  - You're going to need to publish a path for **Internal Publishing**, and enter the FQDN for the external Web Services on your Front End pool's load balancer (or the FQDN of the Director pool's load balancer if you have one), an example would be `sfb_pool01.contoso.local`.
  - You should type `/^*` as the path to be published, but you also need to **forward the original host header**.
  - There will be an option for **public or external name** details or information. This is the place where you'll be able to enter:

- **Accept requests**, but it should be for the domain name.
  - For the **Name**, you should enter **lyncdiscover**. (this is the external Autodiscover Service URL). Now, if you're creating a rule for the external Web Services URL on the Front End pool, you'll need to type the FQDN for the external Web Services on your Front End pool (for example, lyncwebextpool01.contoso.com).
  - There will be a **Path** option, and you'll need to enter  $\wedge^*$  here.
  - You'll need to select a **SSL Listener** with your up-to-date public certificate.
  - **Authentication Delegation** should be set to **No delegation**, but direct client authentication **should** be allowed.
  - The rule should be set to **All users**.
  - This should be all the information you need to create this rule and allow you to proceed.
4. You're going to need to ensure that the **original host header** is forwarded.
  5. The **Web Server** ports will need to be set as well, you'll need to do the following:
    - **Redirect requests to HTTP port** and the port number should be **8080**.
    - **Redirect requests to SSL port** and the port number should be **4443**.
  6. When everything's configured, you'll need to save or apply these, and then you'll want to test the rule.

#### Create a web publishing rule for port 80 (Optional)

1. Open your Reverse proxy interface.
2. You'll need to locate where in the interface you create your web publishing rules, and choose the **New** or **Create** option (it may be on a menu or tab, depending on your Reverse proxy configuration). You are looking for the option to create a new web publishing rule.
3. Typically, you will need to enter the following information:
  - **Name**: the name for your rule
  - **Rule Action**: In this case it's an **Allow** rule, you're letting something pass through your Reverse proxy.
  - The **Publishing** rule or option you're choosing would be **single web site or load balancer**.
  - This needs to be a **non-secured connection to connect to the published Web server or farm**.
  - You're going to need to publish a path for **Internal Publishing**, and enter the FQDN for the **VIP address** of your Front End pool's load balancer, an example would be sfb\_pool01.contoso.local.
  - You should type  $\wedge^*$  as the path to be published, but you also need to **forward the original host header**.
  - There will be an option for **public or external name** details or information. This is the place where you'll be able to enter:
    - **Accept requests**, but it should be for the domain name.
    - For the **Name**, you should enter **lyncdiscover**. (this is the external Autodiscover Service URL).
    - There will be a **Path** option, and you'll need to enter  $\wedge^*$  here.
    - You'll need to select a web listener, or allow your Reverse proxy to create one for you.

- **Authentication Delegation** should be set to **No delegation**, but direct client authentication **should not** be allowed.
  - The rule should be set to **All users**.
  - This should be all the information you need to create this rule and allow you to proceed.
4. The **Web Server** ports will need to be set, you'll need to do the following:
- **Redirect requests to HTTP port** and the port number should be **8080**.
  - **Redirect requests to SSL port** and the port number should be **4443**.
5. When everything's configured, you'll need to save or apply these, and then you'll want to test the rule.

## Configure Autodiscover for Mobility with hybrid deployments

Hybrid environments in Skype for Business Server are environments that combine an on-premises and O365 environment. When you have Skype for Business Server working in a Hybrid environment, the Autodiscover service needs to be able to locate a user from either of these environments.

To let mobile clients discover where a user's located, the Autodiscover service needs to be configured with a new uniform resource locator (URL). The steps are:

1. Open Skype for Business Server Management Shell.
2. Run the following to get the value of the attribute **ProxyFQDN** for your Skype for Business Server environment:

```
Get-CsHostingProvider
```

3. Then, still in the shell window, run:

```
Set-CsHostingProvider -Identity [identity] -AutodiscoverUrl  
https://webdir.online.lync.com/autodiscover/autodiscover.service.svc/root
```

Where [identity] is replaced with the domain name of the shared SIP address space.

## Test your Mobility deployment

Once you've deployed Skype for Business Server Mobility Service and Skype for Business Server Autodiscover Service, you'll want to run a test transaction, to make sure your deployment's working right. You can run **Test-CsUcwaConference** to test the ability of two users to create, join and communicate in a conference. You will need two users (real or test) and their full credentials to do this testing. This command will work for both Skype for Business clients as well as Lync Server 2013 clients.

For Lync Server 2010 clients on Skype for Business Server 2015, you'll need to run **Test-CsMcxP2PIM** to test. Your Lync Server 2010 users will still have to be actual users, or predefined test users, and you'll need their password credentials.

### NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## Test conferencing for Skype for Business and Lync 2013 mobile clients

1. Log on as a member of the **CsAdministrator** role on any computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell** (you might type the name in search or go to **All Programs** and choose it).
3. At the command line, enter:

```
Test-CsUcwaConference -TargetFqdn <FQDN of Front End pool> -Authentication <TrustedServer | Negotiate | ClientCertificate | LiveID> -OrganizerSipAddress sip:<SIP address of test user 1> -OrganizerCredential <test user 1 credentials> -ParticipantSipAddress sip:<SIP address of test user 2> -ParticipantCredential <test user 2 credentials> -v
```

It's also possible to set credentials in a script and pass them to the test cmdlet. We have an example of this below.

```
$passwd1 = ConvertTo-SecureString "Password01" -AsPlainText -Force
$passwd2 = ConvertTo-SecureString "Password02" -AsPlainText -Force
$testuser1 = New-Object Management.Automation.PSCredential("contoso\UserName1", $passwd1)
$testuser2 = New-Object Management.Automation.PSCredential("contoso\UserName2", $passwd2)
Test-CsUcwaConference -TargetFqdn pool01.contoso.com -Authentication Negotiate -OrganizerSipAddress sip:UserName1@contoso.com -OrganizerCredential $testuser1 -ParticipantSipAddress sip:UserName2@contoso.com -ParticipantCredential $testuser2 -v
```

## Test conferencing for Lync 2010 mobile clients

### NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

1. Log on as a member of the **CsAdministrator** role on any computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell** (you might type the name in search or go to **All Programs** and choose it).
3. At the command line, enter:

```
Test-CsMcp2PIM -TargetFqdn <FQDN of Front End pool> -Authentication <TrustedServer | Negotiate | ClientCertificate | LiveID> -SenderSipAddress sip:<SIP address of test user 1> -SenderCredential <test user 1 credentials> -ReceiverSipAddress sip:<SIP address of test user 2> -ReceiverCredential <test user 2 credentials> -v
```

It's also possible to set credentials in a script and pass them to the test cmdlet. We have an example of this below.

```
$passwd1 = ConvertTo-SecureString "Password01" -AsPlainText -Force
$passwd2 = ConvertTo-SecureString "Password02" -AsPlainText -Force
$tuc1 = New-Object Management.Automation.PSCredential("contoso\UserName1", $passwd1)
$tuc2 = New-Object Management.Automation.PSCredential("contoso\UserName2", $passwd2)
Test-CsMcp2PIM -TargetFqdn pool01.contoso.com -Authentication Negotiate -SenderSipAddress sip:UserName1@contoso.com -SenderCredential $tuc1 -ReceiverSipAddress sip:UserName2@contoso.com -ReceiverCredential $tuc2 -v
```



To review the command procedures further, you can check out [Test-CsUcwaConference](#) and [Test-CsMcxP2PIM](#).

## Configure for push notifications

Push notifications, in the form of badges, icons, or alerts, can be sent to a mobile device even when the Skype or Lync app is inactive. But what are push notifications? They are event alerts, like a new or missed IM invitation, or for a received voicemail. The Skype for Business Server Mobility service sends these notifications to the cloud-based Skype for Business Server Push Notification Service, which then sends the notifications to the Microsoft Push Notification Service (MSNS) for Windows Phone users.

This functionality is unchanged from Lync Server 2013, but if you have a Skype for Business Server, you'll want to do the following:

- For a Skype for Business Server Edge Server, add a new hosting provider, Microsoft Skype for Business Online, and then set up hosting provider federation between your organization and Skype for Business Online.
- Enable push notifications by running the **Set-CsPushNotificationConfiguration** cmdlet. By default, push notifications are turned off.
- Test your federation configuration and push notifications.

### Configure your Skype for Business Edge Server for push notifications

1. Log on, with an account that's a member of the **CsAdministrator** role, to a computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell**.
3. Add a Skype for Business Server online hosting provider.

```
New-CsHostingProvider -Identity <unique identifier for hosting provider> -Enabled $True -ProxyFQDN <FQDN for the Access Server used by the hosting provider> -VerificationLevel UseSourceVerification
```

As an example:

```
New-CsHostingProvider -Identity "SkypeOnline" -Enabled $True -ProxyFQDN "sipfed.online.lync.com" -VerificationLevel UseSourceVerification
```

#### NOTE

You can't have more than one federation relationship with a single hosting provider. So, if you've already set up a hosting provider that has a federation relationship with sipfed.online.lync.com, don't add another hosting provider for it, even if the identity of the hosting provider is something other than SkypeOnline.

4. Set up the hosting provider federation between your organization and the Push Notification Service at Skype for Business Online. At the command line, you'll need to type:

```
New-CsAllowedDomain -Identity "push.lync.com"
```

### Enable push notifications

1. Log on, with an account that's a member of the **CsAdministrator** role, to a computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell**.

### 3. Enable push notifications:

```
Set-CsPushNotificationConfiguration -EnableMicrosoftPushNotificationService $True
```

### 4. Enable Federation:

```
Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
```

## Test federation and push notifications

1. Log on, with an account that's a member of the **CsAdministrator** role, to a computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell**.
3. Test the federation configuration:

```
Test-CsFederatedPartner -TargetFqdn <FQDN of Access Edge server used for federated SIP traffic> -Domain <FQDN of federated domain> -ProxyFqdn <FQDN of the Access Edge server used by the federated organization>
```

As an example:

```
Test-CsFederatedPartner -TargetFqdn accessproxy.contoso.com -Domain push.lync.com -ProxyFqdn sipfed.online.lync.com
```

### 4. Test your push notifications:

```
Test-CsMcxPushNotification -AccessEdgeFqdn <Access Edge service FQDN>
```

As an example:

```
Test-CsMcxPushNotification -AccessEdgeFqdn accessproxy.contoso.com
```

## Configure Mobility policy

You have the ability with Skype for Business Server to determine who can use your Mobility service, Call via Work, voice over IP (VoIP), or video, as well as whether WiFi will be required for VoIP or video. Call via Work lets a mobile user use their work phone number, instead of their mobile phone number, when placing and receiving calls. The person on the other end of the line won't see that mobile user's cell phone number, and it lets that mobile user avoid outgoing call charges. When VoIP and video are set up, users can take and make VoIP calls and video. The settings for WiFi usage determine whether a user's mobile device will be required to use a WiFi network over a cellular data network.

Mobility, Call via Work, and the VoIP and video features are all enabled by default. The setting to require WiFi for VoIP and video are disabled. An Admin has the ability to change this, either globally, by site, or by user.

To be able to use Mobility features and Call via Work, users need to be:

- Enabled for Skype for Business Server
- Enabled for Enterprise Voice.
- Assigned a Mobility policy that has the **EnableMobility** option set to **True**.

For users to be able to use Call via Work, they'll also need to be:

- Assigned a voice policy that has the **Enable simultaneous ringing of phones** option selected.
- Assigned a Mobility policy that has the **EnableOutsideVoice** set to **True**.

#### NOTE

Users who aren't enabled for Enterprise Voice can use their mobile devices to make Skype to Skype VoIP calls or can join conferences by using the Click to Join link while on their mobile devices, if the appropriate options are set for the Voice policy they're associated with. There's more detail in the PLANNING topic.

### Modify global Mobility policy

1. Log on, with an account that's a member of the **CsAdministrator** role, to a computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell**.
3. Turn off access to Mobility and Call via Work globally by typing:

```
Set-CsMobilityPolicy -EnableMobility $False -EnableOutsideVoice $False
```

#### NOTE

You can turn off Call via Work without turning off access to Mobility. But you can't turn off Mobility without also turning off Call via Work.

For more info, check out [Set-CsMobilityPolicy](#).

### Modify Mobility policy by site

1. Log on, with an account that's a member of the **CsAdministrator** role, to a computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell**.
3. You can create a site-level policy, turn off VoIP and video, enable Require WiFi for IP Audio, and Require WiFi for IP Video by site. Type:

```
New-CsMobilityPolicy -Identity site:<site identifier> -EnableIPAudioVideo $false -RequireWiFiForIPAudio $True -RequireWiFiforIPVideo $True
```

Learn more at [New-CsMobilityPolicy](#).

### Modify Mobility policy by user

1. Log on, with an account that's a member of the **CsAdministrator** role, to a computer where **Skype for Business Server Management Shell** and **Ocscore** are installed.
2. Start the **Skype for Business Server Management Shell**.
3. Create user level Mobility policies and turn off Mobility and Call via Work by user. Type:

```
New-CsMobilityPolicy -Identity <policy name> -EnableMobility $False -EnableOutsideVoice $False  
Grant-CsMobilityPolicy -Identity <user identifier> -PolicyName <policy name>
```

A further example with sample data:

```
New-CsMobilityPolicy "tag:disableOutsideVoice" -EnableOutsideVoice $False  
Grant-CsMobilityPolicy -Identity MobileUser1@contoso.com -PolicyName tag:disableOutsideVoice
```

**NOTE**

You can turn off Call via Work without turning off access to Mobility. But you can't turn off Mobility without also turning off Call via Work.

# Deploy clients for Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Overview of enterprise client installation methods for Skype for Business.

How you deploy Skype for Business to your users depends on whether you purchased Skype for Business as part of an Office 365 plan or you purchased a volume licensed version of Skype for Business.

- **Office 365** If you have an Office 365 plan that includes Skype for Business, the installation technology that's used is called Click-to-Run. With Office 365, you can let your users install Skype for Business for themselves from the Office 365 portal. Or, you can deploy Skype for Business to your users by downloading the software to your local network and then using your existing software deployment tools, such as with Microsoft System Center Configuration Manager. For installation information about Skype for Business that comes with Office 365, see [Deploy the Skype for Business client in Office 365](#).
- **Volume licensed** If you have a volume licensed version of the Skype for Business 2015 or 2016 client, the installation technology that's used is Windows Installer (MSI). A Windows Installer-based installation package consists of multiple MSI files. A language-neutral core MSI package is combined with one or more language-specific packages to make a complete product. Setup assembles the individual packages and performs customization and maintenance tasks during and after installation of Office on users' computers. The Skype for Business 2019 client uses Click-to-Run installers.

The topics in this section describe how to use and customize the Windows Installer to deploy the Skype for Business client to your users through your normal procedures.

## NOTE

The Skype Meeting Add-in for Microsoft Office, which supports meeting management from within the Outlook messaging and collaboration client, installs automatically with Skype for Business clients.

## NOTE

The Office 365 setup program does not uninstall previous versions of Lync. The Skype for Business client installs side-by-side with other Lync clients.

## Installing Windows clients

- [Customize Windows client installation in Skype for Business Server](#)
- [Configure the client experience with Skype for Business](#)
- [Configure Smart contacts list in Skype for Business Server](#)

## Installing device clients

- [Install and test Skype for Business for Windows Phone](#)
- [Install and test Skype for Business for iOS](#)
- [Deploy the Lync VDI plug-in with Skype for Business Server](#)
- [Deploy Web downloadable clients in Skype for Business Server](#)

- [Customize the Mac client experience in Skype for Business](#)

## See also

[Deploy the Skype for Business client in Office 365](#)

# Customize Windows client installation in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Overview of installation methods and tools for Skype for Business.

## NOTE

For installation information about Skype for Business that comes with Office 365, see [Deploy the Skype for Business client in Office 365](#).

Enterprise administrators can customize the Windows Installer-based (.msi) installation of volume licensed versions of Skype for Business by using the methods discussed in this section. Because no single tool provides all customization options, you'll likely use a combination of these methods in your Skype for Business deployment. You might use the tools described in the following sections:

- [Use the Office Customization Tool \(OCT\) in Skype for Business Server](#) to customize setup options and features for Skype for Business and other Office programs.
- [Use Config.xml to perform installation tasks in Skype for Business Server](#) to specify the path of the network installation point and perform silent installation.
- [Use Setup command-line options in Skype for Business Server](#) to specify the Config.xml file to use during installation.
- [Configure client bootstrapping policies in Skype for Business Server](#) by using the Group Policy Object Editor MMC snap-in.

There will probably be other options you'll want to configure as you deploy the Office suite of products. The topics in this section give an overview of these customization tools and discuss considerations specific to Skype for Business. Included are links to detailed Office help for each tool.

# Use the Office Customization Tool (OCT) in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** How to use the Office Customization Tool with the Skype for Business client.

The Office Customization Tool (OCT) is part of the Setup program and is the recommended tool for many customizations. By using the OCT, you customize Office and save your customizations in a Setup customization .msp file. You place the file in the Updates folder on the network installation point. When you install Office, Setup looks for a Setup customization file in the Updates folder and applies the customizations. The Updates folder can be used only to deploy software updates during an initial installation of Office.

The OCT is part of setup and it is only used for volume licensed versions of the product. You run the OCT by typing `setup.exe /admin` at the command line from the root of the network installation point that contains the Office source files. For example, use the following:

```
\\server\share\Office15\setup.exe /admin
```

Administrators use the OCT to create a setup customization .msp file and can customize the following areas:

- **Setup** Used to specify default installation location on the client and default organization name, additional network installation sources, product key, end-user license agreement, display level, earlier versions of Office to remove, custom programs to run during installation, security settings, and Setup properties.
- **Features** Used to configure user settings and to customize how Office features are installed. Administrators can use the OCT to specify initial default values of Office application settings for users. Users can modify most of the settings after the installation.
- **Additional content** Used to add or remove files, add or remove registry entries, and configure shortcuts.
- **Outlook** Used to customize a user's default Outlook profile, specify Exchange settings, add accounts, remove accounts and export settings, and specify Send\Receive groups.

For information about the OCT, see [Use the OCT to customize Office 2013](#). Note that this information also applies to later versions of Office.



# Use Config.xml to perform installation tasks in Skype for Business clients

8/7/2019 • 2 minutes to read

**Summary:** How to use the Config.xml file to specify additional installation instructions.

Although the Office Customization Tool (OCT) is the primary tool for customization installation, administrators can use the Config.xml file to specify additional installation instructions that are not available in the OCT. The following customizations can only be made by using the Config.xml file:

- Specify the path of the network installation point.
- Select the products to install.
- Configure logging and the location of the Setup customization file and software updates.
- Specify installation options, such as user name.
- Copy the local installation source (LIS) to the user's computer without installing Office.
- Add or remove languages from the installation.

We recommend that you use the Config.xml file to configure Skype for Business silent installation.

By default, the Config.xml file that is stored in the core product folder (for example, `\product.WW`) directs Setup to install that product. For example, the Config.xml file in the following folder installs Skype for Business:

- `\server\share\Skype15\Skype.WW\Config.xml`

The Config.xml elements most commonly used for Skype for Business installation are listed in the following table.

## Config.xml elements

ELEMENT	DESCRIPTION
Configuration	Top-level element (required). Contains the Product attribute, for example: Product=Lync (This will work for Skype for Business clients)
OptionState	Specifies how specific product features are handled during installation. Use the following attributes to prevent installation of Business Connectivity Services, which includes shared components that interfere with Outlook: Id="LOBiMain" State="Absent" Children="Force"
Display	The level of UI that Setup displays to the user. Typical attributes include the following: CompletionNotice="Yes"
Logging	Options for the kind of logging that Setup performs. Typical attributes include the following: Type="Off"

ELEMENT	DESCRIPTION
Setting	Specifies values for Windows Installer properties. Typical attributes include the following: Setting Id=" <i>name</i> " (the name of the Windows Installer property) Value=" <i>value</i> " (the value to assign to the property)
DistributionPoint	The fully qualified path of the network installation point from which the installation is to run. Includes the Location attribute: Location=" <i>path</i> "

The following example shows a Config.xml file for a typical silent installation of the Skype for Business client.

```
<Configuration Product="Lync">
  <OptionState Id="LOBiMain" State="Absent" Children="Force" />
  <Display Level="None" CompletionNotice="No" AcceptEula="Yes" />
  <Logging Type="verbose" Path="%temp%" Template="LyncSetupVerbose(*).log" />
  <Setting Id="SETUP_REBOOT" Value="Never" />
  <DistributionPoint Location="\\server\share\Skype15" />
</Configuration>
```

Detailed information about using the Config.xml file to perform Office installation and maintenance tasks is available at <https://go.microsoft.com/fwlink/p/?linkid=267514>.

## To customize the Config.xml file

1. Open the Config.xml file by using a text editor tool, such as Notepad.
2. Locate the lines that contain the elements you want to change.
3. Modify the element entry with the silent options that you want to use. Make sure that you remove the comment delimiters, "`<!--`" and "`-->`". For example, use the following syntax:

```
< distributionpoint="" location="\\server\share\Skype15">
```

4. Save the Config.xml file.

# Use Setup command-line options with Skype for Business clients

8/7/2019 • 2 minutes to read

**Summary:** Learn about Setup.exe command line operations in Office setup.

The Setup.exe command line is used for very few operations in Office setup. Instead of using the Setup command-line options, you'll typically use the Office Customization Tool and the Config.xml file for product setup and feature customization.

The Office Setup.exe command line recognizes the command-line options described in the following table.

## Office Setup Command-Line Options

SETUP COMMAND-LINE OPTION	DESCRIPTION
/admin	Runs the Office Customization Tool to create a Setup customization file (.msp file).
/adminfile [path]	Applies the specified Setup customization file to the installation. You can specify a path of a specific customization file (.msp file) or to the folder where you store customization files.
/config [path]	Specifies the Config.xml file that Setup uses during the installation. Use the /config option to specify the Config.xml file you customized for Skype for Business installations, for example: <code>/config \\server\share\Skype15\Skype.WW\Config.xml</code>
/modify Skype	Used with a modified Config.xml file to run Setup in maintenance mode and make changes to an existing Office installation. For example, you can use the /modify option to add or remove Skype for Business features.
/repair Skype	Runs Setup from the user's computer to repair Skype for Business.
/uninstall Skype	Runs Setup to remove Skype for Business from the user's computer.

# Configure client bootstrapping policies

8/7/2019 • 4 minutes to read

**Summary:** How to manage Group Policies.

The Group Policy Management Console (GPMC) and the Group Policy Object Editor are tools that you use to manage Group Policy. Included with the Office Group Policy Administrative Template are lync16.admx (ADMX) and .adml (ADML) Administrative Templates, which contain the registry-based policy settings for Skype for Business that you configure for Group Policy objects in the domain. ADML files are language-specific complements to ADMX files. Each ADMX and ADML file contains the policy settings for a single Office application. You can [download the Office 2016 Administrative Template files \(ADMX/ADML\)](#) for free from the Microsoft Download Center.

For Skype for Business clients, there are several client bootstrapping policies that you should consider configuring before users sign in to the server for the first time. For example, the default servers and security mode that the client should use until sign-in is complete. You can use Group Policy to establish these settings in users' computer registries before they sign in and begin receiving in-band provisioning settings from the server. The following table lists the Group Policy settings that are available for Skype for Business.

## Group Policy Settings for Skype for Business

GROUP POLICY SETTING	DESCRIPTION
Specify Server (ConfigurationMode)	Specifies how Skype for Business identifies the transport and server to use during sign-in. Within this setting, you specify the following: ServerAddressExternal: Specifies the server name or IP address used by clients and federated contacts when connecting from outside the external firewall. ServerAddressInternal: Specifies the server name or IP address used when clients connect from inside the organization's firewall. Transport: Specifies either Transmission Control Protocol (TCP) or Transport Layer Security (TLS).
Additional server versions supported (ConfiguredServerCheckValues)	Specifies a list of server version names separated by semi-colons that Skype for Business Server will log on to, in addition to the server versions that are supported by default.
Disable automatic upload of sign-in failure logs (DisableAutomaticSendTracing)	Automatically uploads sign-in failure logs to Skype for Business Server for analysis. No logs are automatically uploaded if sign-in is successful. If this policy is not configured, the following happens: For Skype for Business Online users: Sign-in failure logs are automatically uploaded. For Skype for Business on-premises users: A confirmation dialog box is shown to the user before upload. When this setting is disabled, sign-in logs are automatically uploaded to the Skype for Business Server for both Skype for Business on-premises and Skype for Business Online users. When this setting is enabled, sign-in logs are never uploaded automatically.

GROUP POLICY SETTING	DESCRIPTION
Disable HTTP fallback for SIP connection (DisableHttpConnect)	Prevents Skype for Business Server from trying to connect to the server by using HTTP, if TLS or TCP are unavailable. By default, Skype for Business first attempts to connect to the server by using TLS or TCP and, if neither of these transport methods is successful, Skype for Business tries to connect by using HTTP. Use this policy to disable the fallback HTTP connection attempt.
Require logon credentials (DisableNTCredentials)	Requires the user to provide logon credentials for Skype for Business rather than automatically using Windows credentials during sign-in to a SIP server.
Disable server version check (DisableServerCheck)	If you set this policy to 1, prevents Skype for Business from checking the server name and version before signing in. By default, Skype for Business makes these checks before signing in.
Enable using BITS to download Address Book Service files (EnableBitsForGalDownload)	Enables Skype for Business to use Background Intelligent Transfer Service (BITS) to download the Address Book Services files.
Configure SIP security mode (EnableSIPHighSecurityMode)	Enables Skype for Business to send and receive instant messages more securely. This policy has no effect on Windows .NET or Microsoft Exchange Server services. If you do not configure this policy setting, Skype for Business can use any transport. But if it does not use TLS and if the server authenticates users, Skype for Business must use either NTLM or Kerberos authentication.
Global Address Book Download Initial Delay (GalDownloadInitialDelay)	Specifies the time period before a download of the global address list (GAL) occurs. The default value is 60 minutes, which means the server delays the download of GAL file for a random period of between 0 and 60 minutes.
Prevent users from running Skype for Business (PreventRun)	Prevents users from running Skype for Business. You can configure this policy setting under both Computer Configuration and User Configuration, but the policy setting under Computer Configuration takes precedence.
Allow storage of user passwords (SavePassword)	Enables Skype for Business to store passwords.
Configure SIP compression mode (SipCompression)	Specifies when to turn on SIP compression. By default, SIP compression is enabled based on the adapter speed. Note that setting this policy might cause an increase in sign-in time.
Trusted Domain List (TrustModelData)	Lists the trusted domains that do not match the prefix of the customer SIP domain.

Policies configured on the server take precedence over Group Policy settings and client options configured by the user. The following table summarizes the order in which settings take precedence when a conflict occurs.

### Group Policy Precedence

PRECEDENCE	LOCATION OR METHOD OF SETTING
1	Skype for Business Server in-band provisioning

PRECEDENCE	LOCATION OR METHOD OF SETTING
2	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\16.0\Lync
3	HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\16.0\Lync
4	The Options dialog box in Skype for Business

### To define Group Policy settings by using the Skype for Business administrative template files

1. Create a root-level folder to contain all language-neutral ADMX files. For example, create the root folder for the central store on your domain controller at this location:

```
%systemroot%\sysvol\domain\policies\PolicyDefinitions
```

#### NOTE

This procedure assumes that you want to manage multiple computers in your domain. In this case, you store the templates in a central store in the Sysvol folder on the primary domain controller. This provides a replicated central storage location for domain Administrative Templates.

2. Create a subfolder for each language that you'll use. These subfolders will contain the language-specific ADML resource files. For example, create a subfolder for United States English (EN-US) at this location:

```
%systemroot%\sysvol\domain\policies\PolicyDefinitions\EN-US
```

# Install and test Skype for Business for iOS

8/7/2019 • 2 minutes to read

**Summary:** How to install and test the Skype for Business for iOS app.

The Skype for Business for iOS app brings Skype for Business presence, instant messaging (IM), and voice and video calling to iOS devices. Users with Lync 2013 will either get the updated app automatically or be prompted to update it manually, depending on their user settings. New users can download it from the Apple App Store. The Skype for Business for iOS app is only available on iOS versions 8.0 and later.

## Installing Skype for Business for iOS

1. From your iOS device, tap **App Store**, and search for **Skype for Business for iOS**.
2. Tap **Download** > **Open**.
3. Sign in to the app.

## Verifying mobile client installation

After you sign in successfully, use the following tests to verify that your Skype for Business installation is working correctly on your iOS device.

### Search for a contact in the corporate directory

1. In the Contacts list, tap inside the search bar at the top, and begin typing the name of a contact that exists only in the global address list (GAL).
2. Verify that the contact name appears in the search results.

### Test instant messaging and presence

1. In the Contacts list, tap a contact.
2. Verify that an instant messaging (IM) window appears and that you can type and send an IM.

### Test dial-out conferencing

1. In Outlook, schedule a Skype for Business meeting.
2. On the mobile device, open the meeting invitation.
3. Click the **Join Meeting** button.
4. Answer the call from the conference service and verify that you are connected to the meeting audio.

### Test push notifications

1. On user A's mobile device, sign in to Skype for Business with user A's account.
2. Open another application on the mobile device.
3. On a different client, sign in to Skype for Business with user B's account.
4. Send an IM from user B to user A.
5. Verify that the IM notification appears on user A's mobile device.

# Configure Smart contacts list in Skype for Business clients

8/7/2019 • 2 minutes to read

**Summary:** Learn how to turn on the Smart contacts list feature in the Skype for Business client.

The Smart contacts list feature allows automatic population of contact lists for your end users. Upon first using Skype for Business, your users will automatically see their manager and other people on their team. This feature is turned on by default for Office 365 users, but you must explicitly enable this feature for your on-premises users by configuring the client policy setting.

Keep the following in mind when configuring this feature:

- Users, up to 13, are automatically added to the Smart contacts list in the following order:
  1. Manager
  2. Directs in alphabetical order
  3. Peers in alphabetical order
- The first time a user logs in, a new group, named My Group, is created. The group is automatically populated with people in the user's AD group relationship based on the user alias populated in the Manager field. Note that changes to the AD group membership do not cause updates to My Group after it is initially populated. If a user deletes a contact or the group, neither the contact nor the group are re-created.
- If auto tagging is turned on, contacts in the list will be tagged for presence changes. Auto tagging is turned on by default, but you can choose to turn it off.
- All new users in the group will be informed that they have been added to the contacts list. Users can manually add new members to their My Group or to other groups of their choosing.
- This feature works only for users who are signing in for the first time. If a user has previously signed in from any device—including, for example, any mobile device or a Mac—the feature is not enabled for that user.

## Configure Smart contacts list

To enable the Smart contacts list feature for your users, you will need to perform the following steps:

- Create a new CsClientPolicy entry and add it to the global client policy.
- Make sure that Address Book Search is configured for Web Search only.

### Create a policy entry to enable Smart contacts list

To create a policy entry to enable the Smart contacts list feature, use the [New-CsClientPolicyEntry](#) cmdlet with the `EnableClientAutoPopulateWithTeam` option as follows:

```
$x=New-CsClientPolicyEntry -Name EnableClientAutoPopulateWithTeam -Value $True
```

Next, use the [Set-CsClientPolicy](#) cmdlet to write the changes to the global policy as follows:

```
Set-CsClientPolicy -Identity Global -PolicyEntry @{$Add=$x}
```



You can optionally create a policy to turn off auto tagging as follows:

```
$x=New-CsClientPolicyEntry -Name TagContactsInClientAutoPopulatedGroup -Value $False  
Set-CsClientPolicy -Identity Global -PolicyEntry @{$Add=$x}
```

You must also set the `AddressBookAvailability` parameter for the corresponding policy to `WebSearchOnly`. For more information, see [Set-CsClientPolicy](#).

### Troubleshoot

If Smart contacts list is not functioning as expected, check the following:

- Validate the configuration.
- Confirm that the AD organization information is populated.
- Collect Skype for Business client logs on a new user for further analysis.
- Confirm that the Skype for Business client UI is not displaying a message that it cannot connect to the Address Book. To confirm Address Book connectivity, perform a search for a user in the Skype for Business client search bar.
- AD DS replication issues could cause contacts to be unresolved when a user first signs in to Skype for Business.

# Deploy Web downloadable clients in Skype for Business Server

9/12/2019 • 5 minutes to read

**Summary:** Deploy the Skype for Business 2015 Web App and Skype Meetings App used with Skype for Business Server.

Skype for Business Web App is an Internet Information Services (IIS) web client that is installed on the server running Skype for Business Server and by default it is deployed on demand to meeting users who do not already have the Skype for Business client. These meeting users are more often than not connecting from outside your network. Whenever a user clicks a meeting URL but does not have the Skype for Business client installed, the user is presented with the option to join the meeting by using the latest version of Skype for Business Web App, Skype Meetings App, or Skype for Business for Mac.

The voice, video, and sharing features in Skype for Business Web App require a Microsoft ActiveX control that is used as a plugin by the user's browser. You can either install the ActiveX control in advance or allow users to install it when prompted, which happens the first time they use Skype for Business Web App or the first time they access a feature that requires the ActiveX control.

## NOTE

In Skype for Business Server Edge Server deployments, an HTTPS reverse proxy in the perimeter network is required for Skype for Business Web App client access. You must also publish simple URLs. For details, see [Setting Up Reverse Proxy Servers](#) and [DNS requirements for simple URLs in Skype for Business Server](#).

## Enable Multi-Factor Authentication for Skype for Business Web App

Skype for Business Web App, Skype Meetings App, and Skype for Business for Mac support multi-factor authentication. In addition to user name and password, you can require additional authentication methods, such as smart cards or PINs, to authenticate users who are joining from external networks when they sign in to Skype for Business meetings. You can enable multi-factor authentication by deploying Active Directory Federation Service (AD FS) federation server and enabling passive authentication in Skype for Business Server. After AD FS is configured, external users who attempt to join Skype for Business meetings are presented with an AD FS multi-factor authentication webpage that contains the user name and password challenge along with any additional authentication methods that you have configured.

## IMPORTANT

The following are important considerations if you plan to configure AD FS for multi-factor authentication:

- Multi-factor ADFS authentication works if the meeting participant and organizer are both in the same organization or are both from an AD FS federated organization. Multi-factor ADFS authentication does not work for Lync federated users because the Lync server web infrastructure does not currently support it.
- If you use hardware load balancers, enable cookie persistence on the load balancers so that all requests from the Skype for Business Web App or Meetings App clients are handled by the same Front End Server.
- When you establish a relying party trust between Skype for Business Server and AD FS servers, assign a token life that is long enough to span the maximum length of your Skype for Business meetings. Typically,

a token life of 240 minutes is sufficient.

- This configuration does not apply to Lync mobile clients.

### Configure Multi-Factor Authentication

1. Install an AD FS federation server role. For details, see the [Active Directory Federation Services 2.0 Deployment Guide](#)
2. Create certificates for AD FS. For more information, see "[Federation server certificates](#)" section of the Plan for and deploy AD FS for use with single sign-on topic.
3. From the Windows PowerShell command-line interface, run the following command:

```
add-pssnapin Microsoft.Adfs.powershell
```

4. Establish a partnership by running the following command:

```
Add-ADFSRelyingPartyTrust -Name ContosoApp -MetadataURL  
https://lyncpool.contoso.com/passiveauth/federationmetadata/2007-06/federationmetadata.xml
```

5. Set the following relying party rules:

```
$IssuanceAuthorizationRules = '@RuleTemplate = "AllowAllAuthzRule" => issue(Type =  
"http://schemas.contoso.com/authorization/claims/permit", Value = "true");'$IssuanceTransformRules =  
'@RuleTemplate = "PassThroughClaims" @RuleName = "Sid" c:[Type ==  
"http://schemas.contoso.com/ws/2008/06/identity/claims/primarysid"]=> issue(claim = c);'  
Set-ADFSRelyingPartyTrust -TargetName ContosoApp -IssuanceAuthorizationRules  
$IssuanceAuthorizationRules -IssuanceTransformRules $IssuanceTransformRules  
Set-CsWebServiceConfiguration -UseWsFedPassiveAuth $true -WsFedPassiveMetadataUri  
https://dc.contoso.com/federationmetadata/2007-06/federationmetadata.xml
```

## Disable BranchCache

The BranchCache feature in Windows 7 and Windows Server 2008 R2 can interfere with Skype for Business Web App web components. To prevent issues for Skype for Business Web App users, make sure that BranchCache is not enabled.

For details about disabling BranchCache, see the [BranchCache Deployment Guide](#).

## Verifying Skype for Business Web App Deployment

You can use the Test-CsUcwaConference cmdlet to verify that a pair of test users can participate in a conference using the Unified Communications Web API (UCWA). For details about this cmdlet, see [Test-CsUcwaConference](#) in the Skype for Business Server Management Shell documentation.

## Troubleshooting Plug-in Installation on Windows Server 2008 R2

If installation of the plug-in fails on a computer running Windows Server 2008 R2, you may need to modify the Internet Explorer security setting or the DisableMSI registry key setting.

### Modify the security setting in Internet Explorer

1. Open Internet Explorer.
2. Click **Tools**, click **Internet Options**, and then click **Advanced**.
3. Scroll down to the **Security** section.

4. Clear **Do not save encrypted pages to disk**, and then click **OK**.

**NOTE**

If selected, this setting will also cause an error when trying to download an attachment from Skype for Business Web App.

5. Rejoin the meeting. The plug-in should download without errors.

**Modify the DisableMSI Registry setting**

1. Click **Start**, and then click **Run**.
2. To access the Registry Editor, type **regedit**.
3. Navigate to HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Installer.
4. Edit or add the DisableMSI registry key of type REG\_DWORD and set it to 0.
5. Rejoin the meeting.

## Enable Skype Meetings App to replace Skype for Business Web App (Optional, Skype for Business Server 2015 only)

This procedure is optional, and applies to Skype for Business Server 2015 CU5 and later. If you do not use it, external users will continue to join meetings using Skype for Business Web App.

**Enable simplified meeting join and Skype Meetings App**

1. When you enable access to the Content Delivery Network (CDN), users will have the ability to connect to CDN online and get Skype Meetings App (on Windows) and Skype for Business for Mac (on Mac), and will use the simplified meeting join experience.

```
Set-CsWebServiceConfiguration -MeetingUxUseCdn $True
```

2. Allow client side logging telemetry from the meeting join web page or the Skype Meetings App to be sent to Microsoft servers (the command defaults to false).

```
Set-CsWebServiceConfiguration -MeetingUxEnableTelemetry $True
```

Information sent to Microsoft is in strict compliance with [Skype for Business data collection practices](#).

3. Set the timeout before fall back to the locally hosted Skype for Business Web App experience if CDN isn't available. The default value is 6 seconds. If this value is set to 0, there will be no timeout.

```
Set-CsWebServiceConfiguration -JoinLauncherCdnTimeout (New-TimeSpan -Seconds 10)
```

**NOTE**

With MeetingUxUseCdn in Skype for Business Server 2015 Cumulative Update 5, the default value is set to False. This causes an issue where Skype for Business for Mac client is unable to join non-federated partners' meetings as a guest, even if Skype for Business Admin has set MeetingUxUseCdn to True. For this to work, Skype for Business Server 2015 must have the Cumulative Update 7, 6.0.9319.534, or later. See [Enable Skype Meetings App to replace Skype for Business Web App in Skype for Business Server 2015](#).

## See also

[Plan for Meetings clients \(Web App and Meetings App\)](#)

[Configure the meeting join page in Skype for Business Server](#)

[Microsoft Online Services Privacy Statement](#)

[Licensing Terms and Documentation](#)

# Customize the Mac client experience in Skype for Business

8/8/2019 • 3 minutes to read

This article describes the client preferences and defaults available for the Skype for Business on Mac client, and how to edit them from outside the App.

## Skype for Business on Mac client preference settings

Certain features and behaviors that are available to Skype for Business on Mac clients are determined by preference settings on the client. The Skype for Business on Mac preferences are found in a file located on Macs that have installed the Skype for Business client located at the following path:

**~/Library/Containers/com.microsoft.SkypeForBusiness/Data/Library/Preferences/com.microsoft.SkypeForBusiness.plist**

To set these preferences, get to a terminal prompt on the client's Mac and as needed enter defaults write com.microsoft.SkypeForBusiness key commands using the preference keys described in the following table.

### Client preference keys

KEY	TYPE	VALUE	DESCRIPTION
autoDetectAutoDiscoveryURLs	Bool	0 = manual server configuration 1 = automatic server detection (default)	Specify how Skype for Business identifies the transport and server to use during sign-in. If you enable this policy setting, you must specify <b>internalAutoDiscoveryURL</b> and <b>externalAutoDiscoveryURL</b> .
internalAutoDiscoveryURL	String	Full autodiscover URL	Internal autodiscover URL
externalAutoDiscoveryURL	String	Full autodiscover URL	External autodiscover URL
httpProxyDomain	String		HTTP Proxy Domain
httpProxyUserName	String		HTTP Proxy Username
httpProxyPassword	String		HTTP Proxy Password
trustedDomainList	Array		List of trusted domains for HTTP redirects.
autoAcceptTimeout	Number	300 (default)	Auto-Accept timeout for users without Server-side Conversation History.

KEY	TYPE	VALUE	DESCRIPTION
warnWhenUnknownLocationForE911	Bool	0 = Disabled 1 = Enabled	Warns the user when dialing an emergency number from an unknown location.
sipAddress	String		The SIP address (Email) used to sign-in to Skype for Business.
userName	String		The UPN (UserName) used to sign-in to Skype for Business.
userNameInAdvancedOnly	Bool	0 = display the User Name field on the main sign-in screen and in the Advanced Properties dialog box 1 = display the User Name field only in the Advanced Properties dialog box (default)	Specify where the User Name field is displayed during sign-in.

### Usage examples

To add a single domain (Contoso.com) to the trusted domain list you would use the trustedDomainList key as shown:

```
defaults write com.microsoft.SkypeForBusiness trustedDomainList -array-add "Contoso.com"
```

To add several domains to the trusted domain list you would use the trustedDomainList key as shown:

```
defaults write com.microsoft.SkypeForBusiness trustedDomainList -array-add "sfb.com" "abc.com" "test.org"
```

### Sample unedited settings

For reference, here is a sample settings file using default settings only:

```
{
  BITApplicationDidEnterBackgroundTime = "1496164840.505589";
  BITApplicationWasLaunched = 1;
  CallHistorySelectedFilterIndex = 0;
  HockeySDKAutomaticallySendCrashReports = 0;
  HockeySDKCrashReportActivated = 1;
  "LastSignOut_me" = "2017-05-30 17:22:17 +0000";
  "NSSplitView Subview Frames CallHistoryListDetailSplit" = (
    "0.000000, 0.000000, 291.500000, 473.000000, NO, NO",
    "292.500000, 0.000000, 408.500000, 473.000000, NO, NO"
  );
  "NSSplitView Subview Frames calendarListSplitView" = (
    "0.000000, 0.000000, 320.000000, 473.000000, NO, NO",
    "321.000000, 0.000000, 380.000000, 473.000000, NO, NO"
  );
  "NSSplitView Subview Frames conversationListSplitView" = (
    "0.000000, 0.000000, 320.000000, 473.000000, NO, NO",
    "321.000000, 0.000000, 380.000000, 473.000000, NO, NO"
  );
  "NSWindow Frame HomeWindow" = "511 134 769 473 0 0 1280 778 ";
  "NSWindow Frame SignInWindow" = "388 208 512 518 0 0 1280 778 ";
  RawCameraSupportVersion = 7030;
  appRunning = 1;
  buildTime = "May 22 2017 12:37:28";
  "user@contoso.com_userPreferences" = {
    ContactsListState = {
```

```

        expandedGroupState =          {
            "/me/pendingContacts" = 0;

"/ucwa/v1/applications/414177012058/people/groups/HR6ZQDk_JUI9WUR0Gq0TEAUyFYDk80wzsPAuDxZfjxg=" = 0;
            "/ucwa/v1/applications/414177012058/people/groups/N-
kLDW4VAs403PDv36MNyaYxhuqkRGD1ewpzDGdaHnw=" = 0;
            "/ucwa/v1/applications/414177012058/people/groups/RJk1X9SsFDq-MbvPe2eUyKTdPizt7-eMxij-
ef1SGWQ=" = 0;
            "/ucwa/v1/applications/414177012058/people/groups/Uu1RAGZQL3JnSpYCDqy4KsZCboNF2pqmp-
ru3sqiDPQ=" = 0;

"/ucwa/v1/applications/414177012058/people/groups/Wsbhk91fd80Uv_0aCtHmYPfm0Wal0mzoM5WFbkxaNjM=" = 0;

"/ucwa/v1/applications/414177012058/people/groups/afYHfnLUqTmnwac550aqHUNqLLCqFTZuDezsBeSL0ko=" = 0;
            "/ucwa/v1/applications/414177012058/people/groups/aok8RuCx35GbuVLMp-
_Zi4gnBK_c5q07mANf4Drf8Ak=" = 0;

"/ucwa/v1/applications/414177012058/people/groups/hSrWaq6LwhzvT6sRxyQimwfxzMgLyEc304FgSokesc=" = 0;

"/ucwa/v1/applications/414177012058/people/groups/mDdgShulTTkweoDbjXVp7Y308xM70eFDD2n2j7sAytM=" = 0;
            "/ucwa/v1/applications/414177012058/people/groups/nj3ApLemRK23ChI-
K3x_RRGjlEeqTh6_9w6kYwKwldQ=" = 1;
            "/ucwa/v1/applications/414177012058/people/groups/oRX0pDJ2zEP-
DQ0fynLdvnTEFFNnsV95uvCmVfHjSik=" = 0;
        };
    };
};
    defaultAudioPlaybackDevice = <62706c69 73743030 d4010203 04050618 19582476 65727369 6f6e5824 6f626a65
63747359 24617263 68697665 72542474 6f701200 0186a0a5 07080f10 1155246e 756c6cd3 090a0b0c 0d0e5b64 6973706c
61794e61 6d655624 636c6173 735a6964 656e7469 66696572 80038004 80025f10 5a417070 6c655553 42417564 696f456e
67696e65 3a432d4d 65646961 20456c65 6374726f 6e696373 20496e63 2e202020 2020203a 4d696372 6f736f66 74204c69
66654368 6174204c 582d3330 30303a31 34313030 3030303a 322c315f 101a4d69 63726f73 6f667420 4c696665 43686174
204c582d 33303030 d2121314 155a2463 6c617373 6e616d65 5824636c 61737365 735f1016 4d6f6465 6c2e4175 64696f56
6964656f 44657669 6365a216 175f1016 4d6f6465 6c2e4175 64696f56 6964656f 44657669 6365584e 534f626a 6563745f
100f4e53 4b657965 64417263 68697665 72d11a1b 54726f6f 74800100 08001100 1a002300 2d003200 37003d00 43004a00
56005d00 68006a00 6c006e00 cb00e800 ed00f801 01011a01 1d013601 3f015101 54015900 00000000 00020100 00000000
00001c00 00000000 00000000 00000000 00015b>;
    defaultAudioRecordingDevice = <62706c69 73743030 d4010203 04050618 19582476 65727369 6f6e5824 6f626a65
63747359 24617263 68697665 72542474 6f701200 0186a0a5 07080f10 1155246e 756c6cd3 090a0b0c 0d0e5b64 6973706c
61794e61 6d655624 636c6173 735a6964 656e7469 66696572 80038004 80025f10 5a417070 6c655553 42417564 696f456e
67696e65 3a432d4d 65646961 20456c65 6374726f 6e696373 20496e63 2e202020 2020203a 4d696372 6f736f66 74204c69
66654368 6174204c 582d3330 30303a31 34313030 3030303a 322c315f 101a4d69 63726f73 6f667420 4c696665 43686174
204c582d 33303030 d2121314 155a2463 6c617373 6e616d65 5824636c 61737365 735f1016 4d6f6465 6c2e4175 64696f56
6964656f 44657669 6365a216 175f1016 4d6f6465 6c2e4175 64696f56 6964656f 44657669 6365584e 534f626a 6563745f
100f4e53 4b657965 64417263 68697665 72d11a1b 54726f6f 74800100 08001100 1a002300 2d003200 37003d00 43004a00
56005d00 68006a00 6c006e00 cb00e800 ed00f801 01011a01 1d013601 3f015101 54015900 00000000 00020100 00000000
00001c00 00000000 00000000 00000000 00015b>;
    firstRun = 0;
    showEndCallDialog = 1;
}

```



# Configure your on-premises deployment for Skype Meeting Broadcast

8/7/2019 • 2 minutes to read

**Summary:** Learn about the steps you need to perform to configure Skype Meeting Broadcast for your on-premises Skype for Business Server hybrid deployment.

Skype Meeting Broadcast is an online service that is part of Office 365. If you are running Skype for Business Server on-premises and want to use Skype Meeting Broadcast in your environment, you'll need to follow the configuration steps in this topic. Before you begin, your environment needs to be configured for hybrid with Skype for Business Online. For more information, see [Plan hybrid connectivity between Skype for Business Server and Skype for Business Online](#) and [Deploy hybrid connectivity between Skype for Business Server and Skype for Business Online](#).

## Configure your hybrid environment for Skype Meeting Broadcast

You'll need to do the following to prepare your environment for Skype Meeting Broadcast:

- Configure federation with Skype for Business Online resources
- Configure SIP federated domains

### Configure federation with Skype for Business Online resources

To enable federation with Skype for Business Online resources, you need to configure External Access for a SIP Federated Provider. To do this by using the Skype for Business Server Control Panel follow these steps:

1. Start the Skype for Business Server Control Panel and select **External Access** on the left.
2. Select **SIP Federated Providers** and click **New**.
3. Configure the new provider with the following settings:

<b>Enable communications with this provider:</b>	Selected
<b>Provider name:</b>	LyncOnlineResources
<b>Access Edge service (FQDN):</b>	sipfed.resources.lync.com
<b>Default verification level:</b>	Allow users to communicate with everyone using this provider.

You can also enable federation with Skype for Business Online resources by running the following cmdlet in the Skype for Business Server Management Shell:

```
New-CsHostingProvider -Identity LyncOnlineResources -ProxyFqdn sipfed.resources.lync.com -VerificationLevel AlwaysVerifiable -Enabled $True -EnabledSharedAddressSpace $True -HostsOCSUsers $True -IsLocal $False
```

### Configure SIP federated domains

Next, you need to add SIP Federated domains to the allowed domain list. Repeat these steps for each of the

domains listed, creating 4 new SIP federated domains. These domains include are for the regional data centers used in Skype for Business Online.

1. Start the Skype for Business Server Control Panel and select **External Access** on the left.
2. Select **SIP Federated Domains** and click **New**.
3. For the **Domain name (or FQDN)**, enter the domain, repeating this procedure for each of the following domains:
  - noameetings.lync.com
  - emeameetings.lync.com
  - apacmeetings.lync.com
  - resources.lync.com

You can also configure the external access for SIP federated domains by running the following cmdlets in the Skype for Business Server Management Shell:

```
New-CsAllowedDomain -Identity "noameetings.lync.com"  
New-CsAllowedDomain -Identity "emeameetings.lync.com"  
New-CsAllowedDomain -Identity "apacmeetings.lync.com"  
New-CsAllowedDomain -Identity "resources.lync.com"
```

Once you've completed these configuration steps you can start using Skype Meeting Broadcast in your deployment. For more information about Skype Meeting Broadcast, see [What is a Skype Meeting Broadcast?](#) and [Skype Meeting Broadcast Admin Guide](#).

# Deploy instant messaging and presence in Skype for Business Server

8/7/2019 • 2 minutes to read

**Summary:** Learn about deployment steps for instant messaging and presence in Skype for Business Server.

## Deployment steps for instant messaging and presence

The planning article for instant messaging and presence walks you through information to plan your deployment. Instant messaging and presence is enabled when you install Skype for Business Server. To learn more about planning instant messaging and presence, see [Plan for instant messaging and presence in Skype for Business Server](#).

In this section you learn about some of the deployment steps that you can customize to fine tune your instant messaging and presence scenarios.

## In this section

[Enable or Disable Offline Instant Messaging \(IM\) in Skype for Business Server](#)

# Enable or Disable Offline Instant Messaging (IM) in Skype for Business Server

8/7/2019 • 2 minutes to read

Learn to enable or disable Offline Instant Messaging (IM) in Skype for Business Server.

## Enable Offline Instant Messaging (IM) in Skype for Business Server

Offline IM is a client side feature built into Skype for Business client (2016 C2R build 16.0.6701.1000 or higher) that leverages Exchange Web Services (EWS) to send messages from the Skype for Business client to a user's Exchange mailbox. Offline IM uses Exchange Web Services (EWS) to send Offline messages from the Skype for Business client to the mailbox of recipient. EWS must be available to the Skype for Business client for Offline messages to be sent. To learn more about planning for instant messaging and presence, see [Plan for instant messaging and presence in Skype for Business Server](#).

### NOTE

If the user's mailbox is hosted in Exchange On-Premises, the Skype for Business client (2016 C2R build 16.0.6920.1000) is required

### To enable or disable Offline IM in Skype for Business Server

1. Open the Skype for Business Server Management Shell.
2. Run the following command to enable Offline IM.

```
Set-CsImConfiguration -EnableOfflineIM $True
```

### NOTE

In Skype for Business Server 2015 CU3, the EnableOfflineIM option is set to \$True by default. To disable, set this value to \$False.

3. Run the following command to confirm the ability to store Offline IM's is set.

```
Get-CsImConfiguration
```

## Offline IM Integration with Exchange

Offline IM will not be available to senders if they have a client policy that disables automatic saving of Offline messages to the conversation history folder (EnableIMAutoArchiving = \$false). There is no mechanism to check if the recipient is able to receive Offline messages.

For Offline messages sent within the same organization they will be received as an email message with message class of IM.Note.MissedConversation and will be included in Outlook **Missed Conversation** folder, as well as conversation history which will be picked up in recent list/conversation history tab in Skype for Business clients.

For Offline messages sent from federated organization they will be received as an email message without

IM.Note.MissedConversation and will not be picked up in the missed conversation or conversation history folders.

## Troubleshooting

There is a two minute timer from when an offline message is sent to when it's picked up and processed. If offline messages can't be processed they will appear in the following directory:

```
%localappdata%\microsoft\office\16.0\lync\SipUserAddress\History Spooler
```

The primary Skype for Business ETL log will contain information about Offline message processing and is your best source for investigation/troubleshooting.

### **NOTE**

An issue has been reported where Offline messages failed to send and the 'Drafts' folder was getting filled with messages. This occurred with Exchange On-Premises mailboxes. The issue has been fixed in all C2R channels as of 6/14/2016.

# Deploy high availability and disaster recovery

8/7/2019 • 2 minutes to read

Skype for Business Server offers high availability with server pooling, disaster recovery with pool pairing, and several modes of Back End Server high availability, including AlwaysOn Availability groups, database mirroring, and SQL failover clustering.

High availability refers to making sure that Skype for Business Server services are available even if one or more servers goes down. Disaster recovery refers to keeping services going in the event of a natural or human-caused disaster, and preserving as much data from before the disaster as possible.

This section tells how to deploy these features, and also covers what steps you can take for high availability and disaster recovery for some of your other server roles.

## NOTE

SQL Mirroring is available in Skype for Business Server 2015 but is no longer supported in Skype for Business Server 2019. The AlwaysOn Availability Groups, AlwaysOn Failover Cluster Instances (FCI), and SQL failover clustering methods are preferred with Skype for Business Server 2019.

## Related sections

[Plan for high availability and disaster recovery in Skype for Business Server](#)

## See also

[Deploy an AlwaysOn Availability Group on a Back End Server in Skype for Business Server](#)

[Deploy paired Front End pools for disaster recovery in Skype for Business Server](#)

[Deploy SQL mirroring for Back End Server high availability in Skype for Business Server 2015](#)

# Deploy an Always On Availability Group on a Back End Server in Skype for Business Server

8/7/2019 • 17 minutes to read

Deploy (install) an Always On Availability Group (AG) in your Skype for Business Server deployment.

How you deploy an AG depends on whether you are deploying it in a new pool, an existing pool that uses mirroring, or an existing pool that currently has no high availability for the Back End database.

## NOTE

Using an AG with a Persistent Chat Server role is not supported.

- [Deploy an Always On Availability Group on a new Front End pool](#)
- [Deploy an Always On Availability Group on an existing pool that uses database mirroring](#)
- [Deploy an Always On Availability Group on an existing pool that does not use database mirroring](#)

## Deploy an Always On Availability Group on a new Front End pool

1. Enable the Failover Clustering feature on all the database servers which will be part of the AG. On each server, do the following

- Open Server Manager and click **Add roles and features**.
- Click **Next** until you reach the **Select features** box. Here, select the **Failover Clustering** check box.
- In the **Add features that are required for Failover Clustering?** box, click **Add Features**.
- Click **Install**.

2. Validate the cluster configuration.

- In Server Manager, click the **Tools** menu and then click **Failover Cluster Manager**.
- Under **Actions** on the right side of the screen, click **Validate Configuration**.
- On the **Before You Begin** page, click **Next**.
- Select the servers to add to the cluster, and then click **Run all tests**.
- In the **Summary** box, check any errors that the wizard reports. Then click **Finish** to complete the validation.

The wizard will probably report several warnings, especially if you are not using shared storage. You are not required to use shared storage. However, if you see any **Error** messages, you must fix those issues before continuing.

3. Create the Windows Server Failover Cluster (WSFC).

- In the **Failover Cluster Management** wizard, right-click **Failover Cluster Management**, then click **Create Cluster**.
- On the **Before You Begin** page, click **Next**.

- Add the cluster name and IP address. When the settings are validated, click **Next**.
  - On the Confirmation page, click **Next**.
  - After the cluster is created, click **Finish**.
4. We recommend that you configure the cluster quorum settings to use a file share witness. To do so, use these steps:
- Right-click the cluster name, click **More Actions**, and click **Configure Cluster Quorum Settings**.
  - In the **Select Quorum Configuration Option** page, click **Select the quorum witness**.
  - In the **Select Quorum Witness** page, click **Configure a file share witness**.
  - In the **Configure File Share Witness** page, type the path of the file share you want to use, and then click **Next**.
  - On the **Confirmation** page, click **Next**.
5. On each server in the cluster, enable the AG feature in SQL Server Configuration Manager.
- Open SQL Server Configuration Manager. In the tree on the left side of the screen, click **SQL Server Services**, then double-click the SQL Server service.
  - In the **Properties** box, select the **AlwaysOn High Availability** tab. Select the **Enable AlwaysOn Availability Groups** check box. Restart the SQL Server service when prompted.
6. Use Topology Builder to create the Front End pool, as explained in [Create and publish new topology in Skype for Business Server](#). When you do, specify the AG as the SQL store for the pool.
7. Create the availability group.
- Open SQL Server Management Studio, and connect to the SQL Server instance.
  - In Object Explorer, expand the **Always On High Availability** folder. Right-click the **Availability Groups** folder and click **New Availability Group Wizard**.
  - If the **Introduction** page appears, click **Next**.
  - In the **Specify Availability Group Name** page, type the name of the Availability group, and click **Next**.
  - In the Select Databases page, select the databases that you want to include in the AlwaysOn Availability Group. Then click **Next**.
- Do not include the **ReportServer**, **ReportServerTempDB**, or Persistent Chat databases in the AlwaysOn Availability Group, as these are not supported in this scenario. You can include all other Skype for Business Server databases in the AlwaysOn Availability Group.
- In the **Specify Replicas** page, click the **Replicas** tab. Then click the **Add Replicas** button, and connect to the other SQL instances that you joined as nodes of the Windows Server Failover Cluster.
  - For each instance, select the **Automatic Failover** and **Synchronous Commit** options. Do not select the **Readable Secondary** option.
  - Click the **Endpoints** tab and verify that **Port Number** is set to 5022.
  - Click the **Listener** tab, and select the **Create an availability group listener** option. Under that option, type a name for the listener, and set the **Port** to 1433 (other ports are not supported for this option).



- Click **Add**, and then in the **IPv4 Address** box, provide your preferred virtual IP address, and then click **OK**.
- In the **Select Initial Data Synchronization** page, select Full, and specify a folder that is accessible to the replicas, and that the SQL Server service account used by both replicas has Write permissions for. Then click **Next**.

This file share will be used temporarily when you initialize the databases. If you are dealing with large databases, we recommend that you manually initialize them in case your network bandwidth cannot accommodate the size of the database backups.

- In the Validation page, verify that all validation checks are successful, then click **Next**.
- In the **Summary** page, verify all settings and click Finish.

8. After the pool and the AG are deployed, perform some final steps to make sure that the SQL logins are on each of the replicas in the AlwaysOn Availability Group.

- Open Topology Builder, select **Download topology from existing deployment**, and click **OK**.
- Expand Skype for Business Server, expand your topology, and expand **SQL Server Stores**. Right-click the SQL store of the new AlwaysOn Availability Group, and click **Edit Properties**.
  - At the bottom of the page, in the **SQL Server FQDN** box, change the value to the FQDN of the Listener of the AG.
- Publish the topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**. Then wait a few minutes for the new topology to replicate.
- Open SQL Server Management Studio, and navigate to the AG. Fail it over to a secondary replica.
- Open Skype for Business Server Management Shell and type the following cmdlet to create the SQL logins on this replica:

```
Install-CsDatabase -Update
```

- Repeat the previous two steps (fail over the group to a secondary replica, then use `Install-CsDatabase -Update`) for each replica in the group.

## Deploy an Always On Availability Group on an existing pool that uses database mirroring

### NOTE

If the pool you are upgrading to an AG hosts the Central Management store for your organization, you must first move the CMS to another pool before you upgrade this pool. Use the `Move-CsManagementServer` cmdlet to move the pool. If you do not have another pool in your organization, you can deploy a Standard Edition server temporarily and move the CMS to this server before you upgrade your pool to the AG.

1. Fail over all data from the mirror to the principal node by opening Skype for Business Server Management Shell and typing the following cmdlet.

```
Invoke-CsDatabaseFailover -PoolFqdn <Pool FQDN> -DatabaseType <DatabaseType> -NewPrincipal "Primary"
```

Repeat this cmdlet for each database type in the pool. You can use the following cmdlet to find all the database types stored in this pool.

```
Get-CsPool -Identity <Pool FQDN>
```

2. Use Topology Builder to remove database mirroring from the pool.
  - Open Topology Builder. In your topology, expand **Enterprise Edition Front End Pools**, right-click the name of the pool, and click **Edit Properties**.
  - For each type of SQL store in the pool, clear the **Enable SQL Store Mirroring** check box.
3. Publish the changed topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**
4. Use SQL Server Management Studio to break the mirror.
  - Open SQL Server Management Studio, navigate to your databases, right-click **Tasks** and click **Mirror**. Then click **Remove Mirroring** and click **OK**.
  - Repeat this for all databases in the pool which will be converted to an AG.
5. Set up the Failover Clustering feature on all the database servers which will be part of the AG. On each server, do the following
  - Open Server Manager and click **Add roles and features**.
  - Click **Next** until you reach the **Select features** box. Here, select the **Failover Clustering** check box.
  - In the **Add features that are required for Failover Clustering?** box, click **Add Features**.
  - Click **Install**.
6. Validate the cluster configuration.
  - In Server Manager, click the **Tools** menu and then click **Failover Cluster Manager**.
  - Under **Actions** on the right side of the screen, click **Validate Configuration**.
  - On the **Before You Begin** page, click **Next**.
  - Select the servers to add to the cluster, and then click **Run all tests**.
  - In the **Summary** box, check any errors that the wizard reports. Then click **Finish** to complete the validation.

The wizard will probably report several warnings, especially if you are not using shared storage. You are not required to use shared storage. However, if you see any **Error** messages, you must fix those issues before continuing.
7. Create the Windows Server Failover Cluster.
  - In the **Failover Cluster Management** wizard, right-click **Failover Cluster Management**, then click **Create Cluster**.
  - On the **Before You Begin** page, click **Next**.
  - Add the cluster name and IP address. When the settings are validated, click **Next**.
  - On the Confirmation page, click **Next**.
  - After the cluster is created, click **Finish**.
8. We recommend that you configure the cluster quorum settings to use a file share witness. To do so, use these steps:

- Right-click the cluster name, click **More Actions**, and click **Configure Cluster Quorum Settings**.
  - In the **Select Quorum Configuration Option** page, click **Select the quorum witness**.
  - In the **Select Quorum Witness** page, click **Configure a file share witness**.
  - In the **Configure File Share Witness** page, type the path of the file share you want to use, and then click **Next**.
  - On the **Confirmation** page, click **Next**.
9. On each server in the cluster, enable the AG feature in SQL Server Configuration Manager.
- Open SQL Server Configuration Manager. In the tree on the left side of the screen, click **SQL Server Services**, then double-click the SQL Server service.
  - In the **Properties** box, select the **AlwaysOn High Availability** tab. Select the **Enable AlwaysOn Availability Groups** check box. Restart the SQL Server service when prompted.
10. Create the availability group.
- Open SQL Server Management Studio, and connect to the SQL Server instance.
  - In Object Explorer, expand the **Always On High Availability** folder. Right-click the **Availability Groups** folder and click **New Availability Group Wizard**.
  - If the **Introduction** page appears, click **Next**.
  - In the **Specify Availability Group Name** page, type the name of the Availability group, and click **Next**.
  - In the **Select Databases** page, select the databases that you want to include in the AlwaysOn Availability Group. Then click **Next**.

Do not include the **ReportServer**, **ReportServerTempDB**, or Persistent Chat databases in the AlwaysOn Availability Group, as these are not supported in this scenario. You can include all other Skype for Business Server databases in the AlwaysOn Availability Group.

- In the **Specify Replicas** page, click the **Replicas** tab. Then click the **Add Replicas** button, and connect to the other SQL instances that you joined as nodes of the Windows Server Failover Cluster.
- For each instance, select the **Automatic Failover** and **Synchronous Commit** options. Do not select the **Readable Secondary** option.
- Click the **Endpoints** tab and verify that **Port Number** is set to 5022.
  - Click the **Listener** tab, and select the **Create an availability group listener** option. Under that option, type a name for the listener, and set the **Port** to 1433 (other ports are not supported for this option).
- Click **Add**, and then in the **IPv4 Address** box, provide your preferred virtual IP address, and then click **OK**.
- In the **Select Initial Data Synchronization** page, select **Full**, and specify a folder that is accessible to the replicas, and that the SQL Server service account used by both replicas has Write permissions for. Then click **Next**.

This file share will be used temporarily when you initialize the databases. If you are dealing with large databases, we recommend that you manually initialize them in case your network bandwidth cannot accommodate the size of the database backups.

- In the **Validation** page, verify that all validation checks are successful, then click **Next**.

- In the **Summary** page, verify all settings and click Finish.
11. Create a new store specifying the AG listener, and specifying the principal of the old mirror as the primary node of the AG.
    - Open Topology Builder. In your topology, expand **Shared Components**, right-click **SQL Server Stores**, and click **New SQL Server Store**.
    - In the **Define New SQL Store** page, first select the **High Availability Settings** check box, and then make sure that SQL AlwaysOn Availability Groups appears in the drop-down box.
    - In the **SQL Server Availability Listener FQDN** box, type the FQDN of the listener you created when you created the availability group.
    - In the **SQL Server FQDN** box, type the FQDN of the primary node of the AG, and then click **OK**. This should be the principal of the old mirror for this store.
  12. Associate the new AG with the Front End pool.
    - In Topology Builder, right-click the pool to associate with the AG, and click **Edit Properties**.
    - Under **Associations**, in the **SQL Server Store** box, select the AG. Select the same group for any other databases in the pool which you want to move to the AG.
    - When you're sure that all needed databases are set to the AG, click **OK**.
  13. Publish the topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**.
  14. Perform some final steps to make sure that the SQL logins are on each of the replicas in the AlwaysOn Availability Group.
    - Open Topology Builder, select **Download topology from existing deployment**, and click **OK**.
    - Expand Skype for Business Server, expand your topology, and expand **SQL Server Stores**. Right-click the SQL store of the new AG, and click **Edit Properties**.
    - At the bottom of the page, in the **SQL Server FQDN** box, change the value to the FQDN of the Listener of the AG.
    - Publish the topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**. Then wait a few minutes for the new topology to replicate.
    - Open SQL Server Management Studio, and navigate to the AG. Fail it over to a secondary replica.
    - Open Skype for Business Server Management Shell and type the following cmdlet to create the SQL logins on this replica:

```
Install-CsDatabase -Update
```

- Repeat the previous two steps (fail over the group to a secondary replica, then use `Install-CsDatabase -Update`) for each replica in the group.

## Deploy an Always On Availability Group on an existing pool that does not use database mirroring

## NOTE

If the pool you are upgrading to an AG hosts the Central Management store for your organization, you must first move the CMS to another pool before you upgrade this pool. Use the `Move-CsManagementServer` cmdlet to move the pool. If you do not have another pool in your organization, you can deploy a Standard Edition server temporarily and move the CMS to this server before you upgrade your pool to the AG.

1. Set up the Failover Clustering feature on all the database servers which will be part of the AG. On each server, do the following
  - Open Server Manager and click **Add roles and features**.
  - Click **Next** until you reach the **Select features** box. Here, select the **Failover Clustering** check box.
  - In the **Add features that are required for Failover Clustering?** box, click **Add Features**.
  - Click **Install**.
2. Validate the cluster configuration.
  - In Server Manager, click the **Tools** menu and then click **Failover Cluster Manager**.
  - Under **Actions** on the right side of the screen, click **Validate Configuration**.
  - On the **Before You Begin** page, click **Next**.
  - Select the servers to add to the cluster, and then click **Run all tests**.
  - In the **Summary** box, check any errors that the wizard reports. Then click **Finish** to complete the validation.

The wizard will probably report several warnings, especially if you are not using shared storage. You are not required to use shared storage. However, if you see any **Error** messages, you must fix those issues before continuing.
3. Create the Windows Server Failover Cluster (WSFC).
  - In the **Failover Cluster Management** wizard, right-click **Failover Cluster Management**, then click **Create Cluster**.
  - On the **Before You Begin** page, click **Next**.
  - Add the cluster name and IP address. When the settings are validated, click **Next**.
  - On the Confirmation page, click **Next**.
  - After the cluster is created, click **Finish**.
4. We recommend that you configure the cluster quorum settings to use a file share witness. To do so, use these steps:
  - Right-click the cluster name, click **More Actions**, and click **Configure Cluster Quorum Settings**.
  - In the **Select Quorum Configuration Option** page, click **Select the quorum witness**.
  - In the **Select Quorum Witness** page, click **Configure a file share witness**.
  - In the **Configure File Share Witness** page, type the path of the file share you want to use, and then click **Next**.
  - On the **Confirmation** page, click **Next**.

5. On each server in the cluster, enable AG in SQL Server Configuration Manager.
  - Open SQL Server Configuration Manager. In the tree on the left side of the screen, click **SQL Server Services**, then double-click the SQL Server service.
  - In the **Properties** box, select the **AlwaysOn High Availability** tab. Select the **Enable AlwaysOn Availability Groups** check box. Restart the SQL Server service when prompted.

6. Create the availability group.

- Open SQL Server Management Studio, and connect to the SQL Server instance.
- In Object Explorer, expand the **Always On High Availability** folder. Right-click the **Availability Groups** folder and click **New Availability Group Wizard**.
- If the **Introduction** page appears, click **Next**.
- In the **Specify Availability Group Name** page, type the name of the Availability group, and click **Next**.
- In the **Select Databases** page, select the databases that you want to include in the AG. Then click **Next**.

Do not include the **ReportServer**, **ReportServerTempDB**, or Persistent Chat databases in the AG, as these are not supported in this scenario. You can include all other Skype for Business Server databases in the AG.

- In the **Specify Replicas** page, click the **Replicas** tab. Then click the **Add Replicas** button, and connect to the other SQL instances that you joined as nodes of the WSFC.
- For each instance, select the **Automatic Failover** and **Synchronous Commit** options. Do not select the **Readable Secondary** option.
- Click the **Endpoints** tab and verify that **Port Number** is set to 5022.
- Click the **Listener** tab, and select the **Create an availability group listener** option. Under that option, type a name for the listener, and set the **Port** to 1433 (other ports are not supported for this option).
- Click **Add**, and then in the **IPv4 Address** box, provide your preferred virtual IP address, and then click **OK**.
- In the **Select Initial Data Synchronization** page, select Full, and specify a folder that is accessible to the replicas, and that the SQL Server service account used by both replicas has Write permissions for. Then click **Next**.

This file share will be used temporarily when you initialize the databases. If you are dealing with large databases, we recommend that you manually initialize them in case your network bandwidth cannot accommodate the size of the database backups.

- In the **Validation** page, verify that all validation checks are successful, then click **Next**.
- In the **Summary** page, verify all settings and click **Finish**.

7. Create a new store specifying the AG listener.

- Open Topology Builder. In your topology, expand **Shared Components**, right-click **SQL Server Stores**, and click **New SQL Server Store**.
- In the **Define New SQL Store** page, first select the **High Availability Settings** check box, and then make sure that SQL AlwaysOn Availability Groups appears in the drop-down box.

- In the **SQL Server Availability Listener FQDN** box, type the FQDN of the listener you created when you created the availability group.
  - In the **SQL Server FQDN** box, type the FQDN of the primary node of the AG, and then click **OK**.
8. Associate the new Always On Availability Group with the Front End pool.
- In Topology Builder, right-click the pool to associate with the AG, and click **Edit Properties**.
  - Under **Associations**, in the **SQL Server Store** box, select the AG. Select the same group for any other databases in the pool which you want to move to the AG.
  - When you're sure that all needed databases are set to the AG, click **OK**.
9. Publish the topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**.
10. Perform some final steps to make sure that the SQL logins are on each of the replicas in the AG.
- Open Topology Builder, select **Download topology from existing deployment**, and click **OK**.
  - Expand Skype for Business Server, expand your topology, and expand **SQL Server Stores**. Right-click the SQL store of the new AG, and click **Edit Properties**.
  - At the bottom of the page, in the **SQL Server FQDN** box, change the value to the FQDN of the Listener of the AG.
  - Publish the topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**. Then wait a few minutes for the new topology to replicate.
  - Open SQL Server Management Studio, and navigate to the AG. Fail it over to a secondary replica.
  - Open Skype for Business Server Management Shell and type the following cmdlet to create the SQL logins on this replica:

```
Install-CsDatabase -Update
```

- Repeat the previous two steps (fail over the group to a secondary replica, then use `Install-CsDatabase -Update`) for each replica in the group.

# Deploy paired Front End pools for disaster recovery in Skype for Business Server

11/25/2019 • 2 minutes to read

You may decide to use paired Front End pools to provide disaster recovery protection, but doing so is not a requirement.

You can easily deploy the disaster recovery topology of paired Front End pools using Topology Builder.

## To deploy a pair of Front End pools

1. If the pools are new and not yet defined, use Topology Builder to create the pools.
2. In Topology Builder, right-click one of the two pools, and then click **Edit Properties**.
3. Click **Resiliency** in the left pane, and then select **Associated Backup Pool** in the right pane.
4. In the box below **Associated Backup Pool**, select the pool that you want to pair with this pool. Only existing pools that are not already paired with another pool will be available to select from.
5. Select **Automatic failover and failback for Voice**, and then click **OK**.

When you view the details about this pool, the associated pool now appears in the right pane under **Resiliency**.

6. Use Topology Builder to publish the topology.
7. If the two pools were not yet deployed, deploy them now and the configuration will be complete. You can skip the final steps in this procedure.

However, if the pools were already deployed before you defined the paired relationship, you must complete the following final steps.

8. On every Front End Server in both pools, run the following:

```
<system drive>\Program Files\Skype for Business Server 2019\Deployment\Bootstrapper.exe
```

This configures other services required for backup pairing to work correctly.

9. Once Bootstrapper finishes installing the required components for backup pairing on every Front end Server in both pools, please be sure to re-apply any existing Cumulative Update that was previously applied on these Front End Servers in both pools and then continue with the next step.
10. From a Skype for Business Server Management Shell command prompt, run the following:

```
Start-CsWindowsService -Name LYNCKBACKUP
```

11. Force the user and conference data of both pools to be synchronized with each other with the following cmdlets:

```
Invoke-CsBackupServiceSync -PoolFqdn <Pool1 FQDN>
```



```
Invoke-CsBackupServiceSync -PoolFqdn <Pool2 FQDN>
```

Synchronizing the data may take some time. You can use the following cmdlets to check the status. Make sure that the status in both directions is in steady state.

```
Get-CsBackupServiceStatus -PoolFqdn <Pool1 FQDN>
```

```
Get-CsBackupServiceStatus -PoolFqdn <Pool2 FQDN>
```

#### NOTE

The **Automatic failover and failback for Voice** option and the associated time intervals in Topology Builder apply only to the voice resiliency features that were introduced in Lync Server. Selecting this option does not imply that the pool failover discussed in this document is automatic. Pool failover and failback always require an administrator to manually invoke the failover and failback cmdlets, respectively.

## See also

[Front End pool disaster recovery in Skype for Business Server](#)

# Migration to Skype for Business Server 2019

8/7/2019 • 2 minutes to read

The topics in this section guide you through the process of migrating to Skype for Business Server 2019. This article covers migrating Lync Server 2013 or Skype for Business Server 2015 to Skype for Business Server 2019.

## IMPORTANT

Throughout the content, we use the term *legacy* to refer to the legacy Lync Server 2013 or Skype for Business Server 2015 that you are migrating to Skype for Business Server 2019.

## IMPORTANT

This guide describes the steps generally required to accomplish each phase of migration. It does not address every possible legacy deployment topology or every possible migration scenario. Therefore, you may not need to perform every step described, or you may need to perform additional steps, depending on your deployment. This guide also provides examples of verification steps. These verification steps are provided to help you understand what you need to look for to ensure that each phase completes successfully as you progress through your migration. Tailor these verification steps to your specific migration process.

This guide provides information specific to upgrading your existing deployment. It does not explain how to change your existing topology. This guide does not cover the implementation of new features. When a detailed procedure is documented elsewhere, this guide directs you to the article or article section.

This article defines terms as specified in the following list.

**migration:** Moving your production deployment from Lync Server 2013 or Skype for Business Server 2015 to Skype for Business Server 2019.

**coexistence:** The temporary environment that exists during migration when some functionality has been migrated to Skype for Business Server 2019 and other functionality still remains on a prior version.

**interoperability:** The ability of your deployment to operate successfully during the period of coexistence.

**legacy:** The system you are migrating away from, which is either Lync Server 2013 or Skype for Business Server 2015.

## In this section

- [Before you begin the migration](#)
- [Phase 1: Plan your migration](#)
- [Phase 2: Prepare for migration](#)
- [Phase 3: Deploy pilot pool](#)
- [Phase 4: Move test users to the pilot pool](#)
- [Phase 5: Add Edge Server to pilot pool](#)
- [Phase 6: Move from pilot deployment into production](#)
- [Phase 7: Complete post-migration tasks](#)

- Phase 8: Decommission legacy pools

# Before you begin the migration

8/7/2019 • 2 minutes to read

Before you begin, we recommend that you read the following articles to familiarize yourself with deploying the corresponding roles.

## In this section

- [Migration process](#)
- [Migration phases](#)

# Migration process

8/7/2019 • 2 minutes to read

The recommended and supported migration procedure for Skype for Business Server 2019 is side-by-side migration. This topic describes why you should use side-by-side migration and also includes information about coexistence testing.

## Side-By-Side Migration

In nearly every migration, you should use the side-by-side migration path. In a side-by-side migration, you deploy a new server with Skype for Business Server 2019 alongside a corresponding server that is running a previous version, and then transfer operations to the new server. If it becomes necessary to roll back to the previous version, you have only to shift operations back to the original servers. Be aware that in this situation any new meetings scheduled with upgraded clients will not work, and the clients would also need to be downgraded.

## Coexistence Testing

After you have deployed Skype for Business Server 2019 in parallel with the previous version, the deployment represents a coexistence testing state of Skype for Business Server 2019 and the previous version. While in this state, it is important to test and ensure that services are started, each site can be administered, and clients can communicate with current and legacy users. Prior to the migration of all users, it is very important that you understand the state of each deployment and ensure that each deployment is functional and working properly. Typically, the coexistence testing phase exists throughout the pilot testing of Skype for Business Server 2019. Legacy users are moved to Skype for Business Server 2019 for a period of time to ensure that application compatibility and features and functions are working properly. After pilot testing, users and applications are moved to the production version of Skype for Business Server 2019, and the legacy pools and applications of the previous version are retired.

# Migration phases

8/7/2019 • 2 minutes to read

In Skype for Business Server 2019, you define sites on your network that contain Skype for Business Server 2019 components. A site is a set of computers that are well-connected by a high-speed, low-latency network, such as a single local area network (LAN) or two networks connected by a high-speed fiber optic network.

A Front End pool is a set of Front End Servers that are configured identically and work together to provide services for a common group of users. A pool provides scalability and failover capability to your users. Each server in a pool must run an identical server role or roles. A Standard Edition server, designed for small organizations, also defines a pool and runs on a single server. This enables you to have Skype for Business Server 2019 functionality for a lesser cost, but does not provide a true high-availability solution.

The following phases describe the process of a pool migration to Skype for Business Server 2019. For multiple sites containing multiple pools, each individual pool should follow this phased approach.

1. [Phase 1: Plan your migration](#)
2. [Phase 2: Prepare for migration](#)
3. [Phase 3: Deploy Skype for Business Server 2019 pilot pool](#)
4. [Phase 4: Move test users to the pilot pool](#)
5. [Phase 5: Add Skype for Business Server 2019 Edge Server to pilot pool](#)
6. [Phase 6: Move from pilot deployment into production](#)
7. [Phase 7: Complete post-migration tasks](#)
8. [Phase 8: Decommission legacy pools](#)

# Phase 1: Plan your migration

8/7/2019 • 2 minutes to read

This section covers planning topics for migrating to Skype for Business Server 2019.

## In this section

- [User migration](#)
- [Migrating Archiving and Monitoring Servers](#)
- [Administering servers after migration](#)
- [Migrating multiple sites and pools](#)
- [Migrating XMPP federation](#)

# User migration

8/7/2019 • 2 minutes to read

A generally accepted best practice for migrations is to create several test users and use them to conduct systems tests. After you have successfully moved and tested those accounts, you should identify a group of pilot production users and move their accounts and conduct validation tests on them. When you get satisfactory results, you can move the rest of your users to the new deployment.

For additional information on enabling users for Skype for Business Server 2019, see the [Deploying Skype for Business Server 2019](#) documentation.



# Migrating Archiving and Monitoring Servers

8/7/2019 • 2 minutes to read

If you deployed Archiving Server and Monitoring Server in your legacy environment, you can deploy these servers in your Skype for Business Server 2019 environment after you migrate your Front End pools. If archiving and monitoring functionality are critical to your organization, however, you should add archiving and monitoring to your Skype for Business Server 2019 pilot pool before you migrate so that the functionality is available during the migration process.

If you want archiving and monitoring functionality during the migration process, keep the following considerations in mind:

- Archiving data and monitoring data are not moved to the Skype for Business Server 2019 deployment. The data you back up prior to decommissioning the legacy environment will be your history of activity in the legacy environment.
- The legacy version of Archiving Server and Monitoring Server can be associated only with a legacy Front End pool. In Skype for Business Server 2019, Archiving and Monitoring are no longer server roles, but services integrated into the Skype for Business Server 2019 Front End pool.
- During the time that your legacy and Skype for Business Server 2019 deployments coexist, the legacy version of Archiving Server and Monitoring Server gather data for users homed on legacy pools. Archiving and Monitoring in Skype for Business Server 2019 gather data for users homed on Skype for Business Server 2019 pools.

## NOTE

During the phase of migration when you are still using your legacy Edge server with the new Skype for Business Server 2019 pilot pool, the legacy version of Archiving Server continues to gather data for users homed on legacy pools and Archiving in Skype for Business Server 2019 gathers data for users homed on Skype for Business Server 2019 pools.

- If you use a third-party archiving and monitoring solution in conjunction with Archiving and Monitoring in Skype for Business Server 2019, consult with your vendor about when and how you need to integrate the third-party solution with Skype for Business Server 2019.

# Administering servers after migration

8/7/2019 • 2 minutes to read

In general, you must use the administrative tool that corresponds to the server version that you want to manage. You cannot install administrative tools from different releases on the same computer.

## **IMPORTANT**

After a Skype for Business Server pilot pool is deployed, you cannot use Topology Builder or Control Panel to manage any 2019 resources. You must use 2019 tools to manage all current and previous version resources.

# Migrating multiple sites and pools

8/7/2019 • 2 minutes to read

Skype for Business Server 2019 supports multi-site and multi-pool deployments. The process of migrating multiple pools to Skype for Business Server 2019 requires the following considerations:

1. After deploying a Skype for Business Server 2019 pilot pool, you need to define a subset of pilot users that will be moved to the Skype for Business Server 2019 pool, and a methodology for validating the functionality of the users. For example, after moving a user to the pilot pool, verify that the user's conference policy has moved to Skype for Business Server 2019.
2. After deploying an Edge Server in the pilot pool, you need to validate that external users can communicate with the Skype for Business Server 2019 pool.
3. Persistent Chat, SQL Mirroring, and XMPP functionality are deprecated in Skype for Business Server 2019 and no longer available as Skype for Business Server 2019 features, but they can be continued in a coexistence environment if they were previously deployed in a legacy environment. If you want to continue using these features, you should plan to continue with a coexistence environment where certain users will remain in legacy pools.
4. After transitioning the federated routes' Edge Servers to the pilot Skype for Business Server 2019 Edge Servers, you need to validate that federated users can communicate with the Skype for Business Server 2019 pool.
5. After moving all users and non-user contact objects, you need to validate that the legacy pool is empty.
6. After verifying that the legacy pool is empty, you can then deactivate the pool.

For details about how to deactivate the legacy pool and servers, see [Phase 8: Decommission legacy pools](#).

# Migrating XMPP federation

8/7/2019 • 2 minutes to read

Previous versions provided an extensible messaging and presence protocol (XMPP) gateway that could be deployed as a separate server role to allow federating with XMPP deployments. The XMPP functionality is no longer available and is deprecated in Skype for Business Server 2019. If you want to continue with the XMPP functionality, you can do so in a coexistence environment with a legacy version (Skype for Business Server 2015 or Lync Server 2013). XMPP functionality is installed in two parts: as an XMPP proxy that runs on the legacy Edge Server, and the XMPP Gateway that runs on the legacy Front End Server.

From a migration perspective, users who want to avail the XMPP feature should remain in the legacy server and should not be moved to a Skype for Business Server 2019 pool but continue to use the legacy XMPP gateway. This is possible only when the XMPP federated partner is configured in Skype for Business Server 2015 or Lync Server 2013. You should not migrate the legacy Edge Server to Skype for Business Server 2019 if you want to continue with XMPP functionality. However, you can have coexistence of the legacy Edge Server (with XMPP Proxy) and the Skype for Business 2019 Edge Server.

# Phase 2: Prepare for migration

8/7/2019 • 2 minutes to read

Before you begin your migration to Skype for Business Server 2019, follow the steps described in this section.

## In this section

- [Apply updates](#)
- [Configure DNS records for pilot pool deployment](#)
- [Back up systems and data](#)
- [Configure clients for migration](#)
- [Verify the legacy environment](#)

# Apply updates

8/7/2019 • 2 minutes to read

Before you migrate, updates must be applied to your environment. For the most up-to-date information, see the **Skype for Business downloads and updates** at <https://go.microsoft.com/fwlink/p/?linkid=232630>.

# Configure DNS records for pilot pool deployment

8/7/2019 • 2 minutes to read

Before deploying the pilot pool, you must update the DNS Host A entries for the pilot pool. To successfully complete this procedure, you should be logged on to the server or domain as a member of the Domain Admins group or a member of the DnsAdmins group.

## To configure DNS Host A records

1. On the Domain Name System (DNS) server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your domain, expand **Forward Lookup Zones**, and then right-click the domain in which Skype for Business Server 2019 will be installed.
3. Click **New Host (A or AAAA)**.
4. Click **Name**, type the host name for the Skype for Business Server 2019 pool (the domain name is assumed from the zone that the record is defined in and does not need to be entered as part of the A record).
5. Click **IP Address**, and then type the IP address for the Front End pool.
6. Click **Add Host**, and then click **OK**.
7. When you are finished, click **Done**.

# Back up systems and data

8/7/2019 • 2 minutes to read

Before you begin the migration, perform a full system backup and document your existing system, including an inventory of user accounts that are homed on each pool, so that you can roll back if it becomes necessary. Multiple tools and programs are available for backing up and restoring data, settings, and systems.

For details and procedures, see [backup and restore procedures](#) for your version.



# Configure clients for migration

8/7/2019 • 2 minutes to read

This topic contains the recommended client deployment steps you should take before migrating to Skype for Business Server 2019. These configuration changes should be made on Lync Server 2013 or Skype for Business Server 2015 (the version you are migrating **from**).

## To configure clients before migration

1. Deploy the most recent server, client, and device updates (hotfixes) for your existing installation.
2. On the previous version of Skype for Business Server, use Client Version Filtering to only allow clients with the most current updates installed.

## See also

[New and changed settings for Lync 2013](#)

[Client interoperability in Lync 2013](#)

[Plan for clients and devices](#)

# Verify the legacy environment

8/7/2019 • 2 minutes to read

Before deploying Skype for Business Server 2019 in a coexistence state, you need to verify that legacy services have been configured and started. It is important to identify key services and features that exist in your legacy environment prior to deploying a Skype for Business Server 2019 pilot pool. Before deploying Microsoft Skype for Business Server 2019 XMPP in a coexistence state with a legacy XMPP deployment, you need to verify that the legacy XMPP services have been configured and started, and identify which federated partner the legacy XMPP configuration is supporting. Verifying your legacy deployment entails the following:

- Verifying that the legacy services are started
- Reviewing the topology and users
- Verifying the federation and Edge server settings
- Verifying XMPP services and federated partners

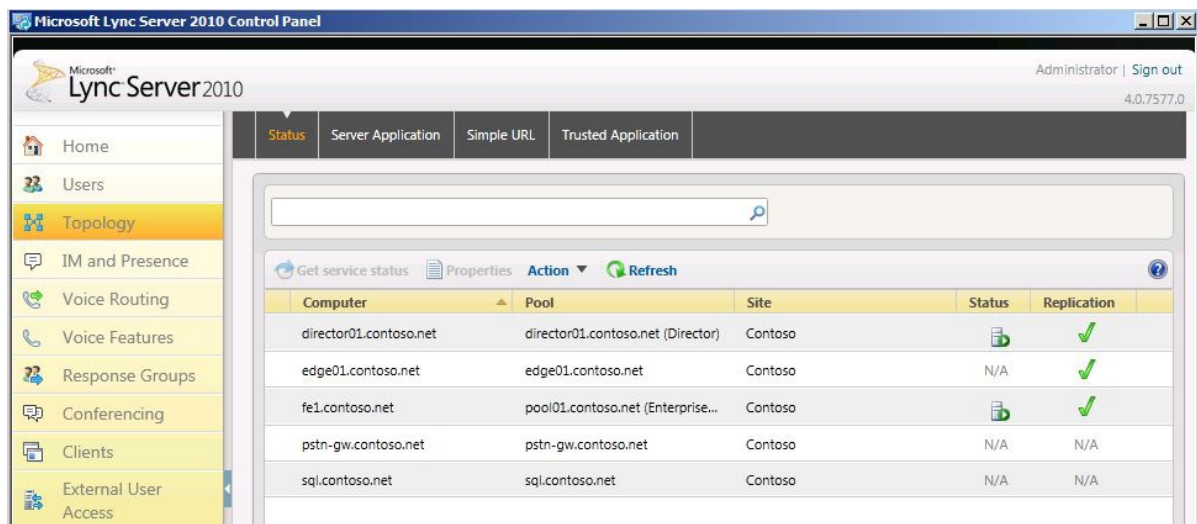
## Verify that legacy services are started

1. From the legacy Front End Server, navigate to the Administrative Tools\Services applet.
2. Verify that the following services are running on the Front End Server:

 Lync Server Application Sharing	Lync Server Application S...	Started	Automatic
 Lync Server Audio Test Service	Lync Server Audio Test S...	Started	Automatic
 Lync Server Audio/Video Conferencing	Lync Server Audio/Video ...	Started	Automatic
 Lync Server Bandwidth Policy Service (Authentication)	Lync Server Bandwidth P...	Started	Automatic
 Lync Server Bandwidth Policy Service (Core)	Lync Server Bandwidth P...	Started	Automatic
 Lync Server Call Park	Lync Server Call Park	Started	Automatic
 Lync Server Conferencing Announcement	Lync Server Conferencing...	Started	Automatic
 Lync Server Conferencing Attendant	Lync Server Conferencing...	Started	Automatic
 Lync Server File Transfer Agent	Lync Server File Transfer ...	Started	Automatic
 Lync Server Front-End	Lync Server Front-End	Started	Automatic
 Lync Server IM Conferencing	Lync Server IM Conferen...	Started	Automatic
 Lync Server Master Replicator Agent	Lync Server Master Replic...	Started	Automatic
 Lync Server Mediation	Lync Server Mediation	Started	Automatic
 Lync Server Replica Replicator Agent	Lync Server Replica Repli...	Started	Automatic
 Lync Server Response Group	Lync Server Response Gr...	Started	Automatic
 Lync Server Web Conferencing	Lync Server Web Confere...	Started	Automatic
 Lync Server Web Conferencing Compatibility	Lync Server Web Confere...	Started	Automatic

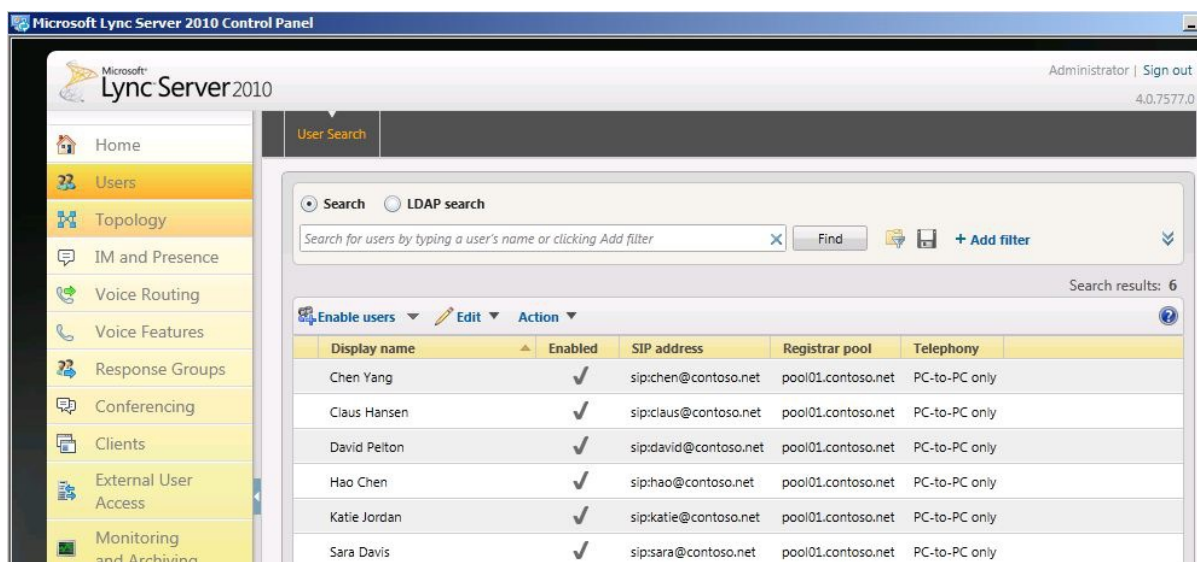
## Review the legacy topology in Skype for Business Server Control Panel

1. Log on to the Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open the Skype for Business Server Control Panel.
3. Select **Topology**. Verify that the various servers in your legacy deployment are listed.



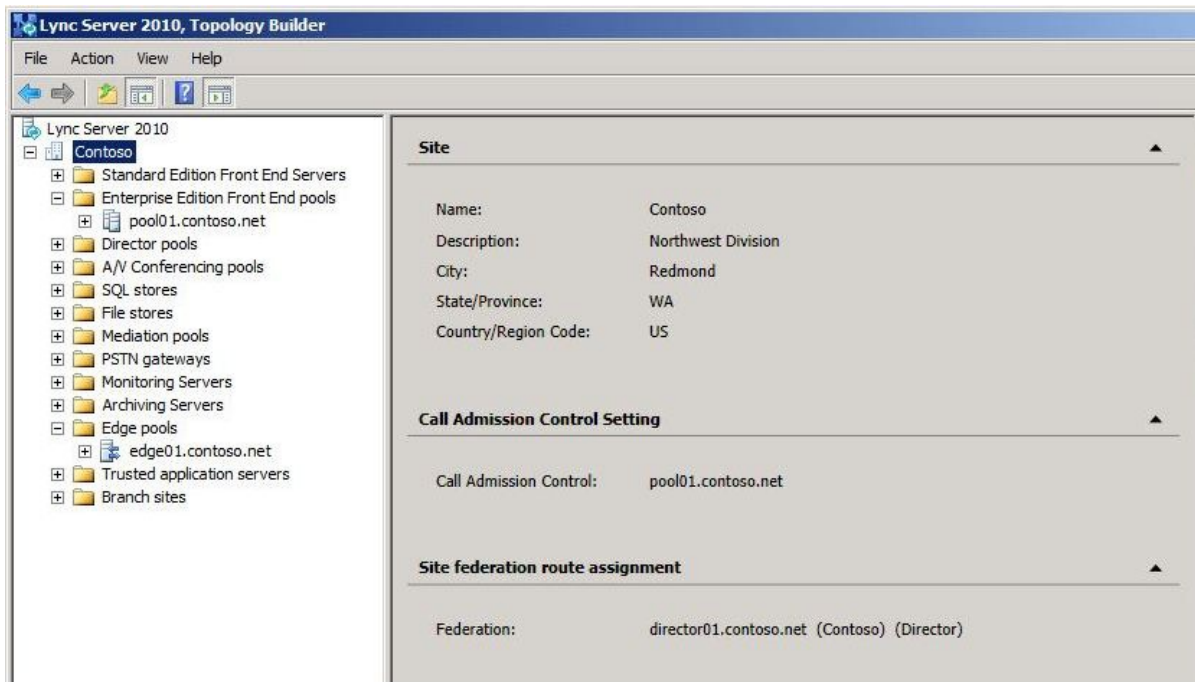
## Review legacy users in Skype for Business Server Control Panel

1. Open the Skype for Business Server Control Panel.
2. Select **Users**, and then click **Find**.
3. Verify that the **Registrar Pool** column points to the legacy pool for each user listed.

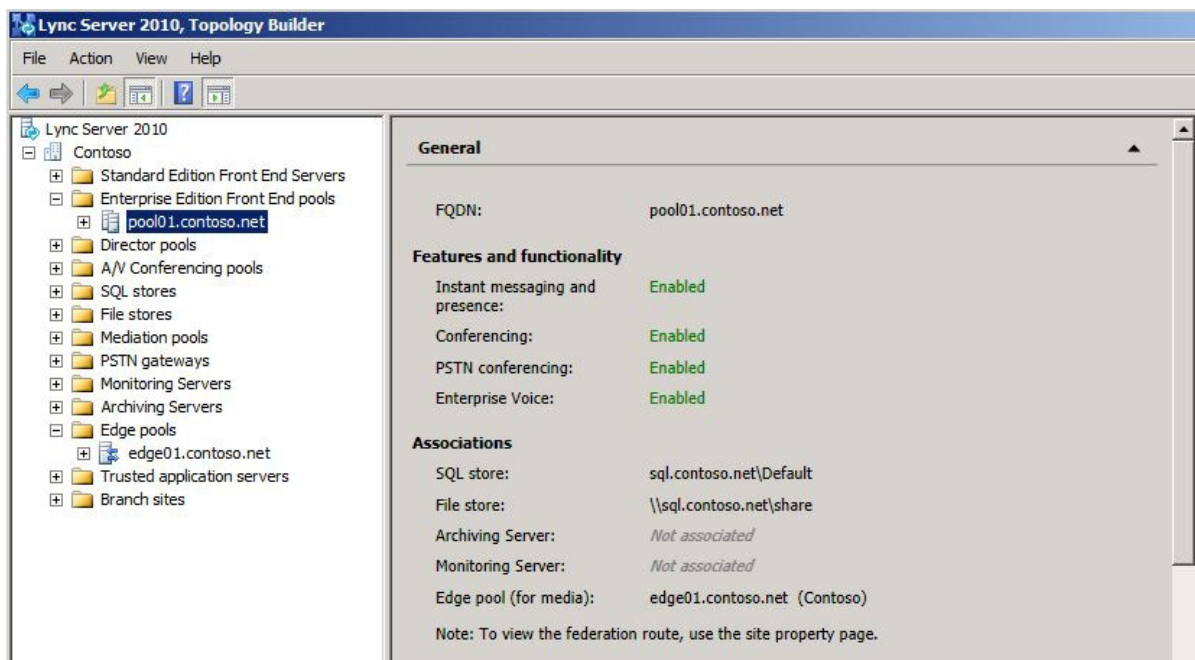


## Verify legacy Edge and federation settings

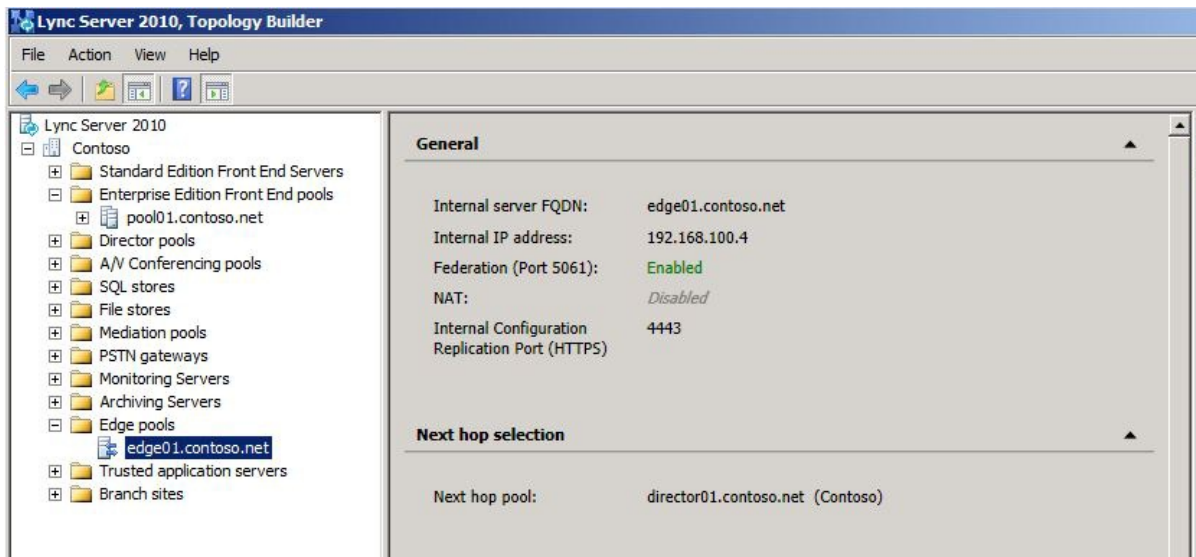
1. Start Topology Builder.
2. Select **Download Topology from existing deployment**.
3. Choose a file name, and save the topology with the default .tbxml file type.
4. Expand the legacy installs node to reveal the various server roles in the deployment.
5. Select the site node and verify that a **Site federation route assignment** value is set.



6. Select the Standard Edition Server or Enterprise Edition front end pool. Determine whether an Edge pool has been configured for media below **Associations**.

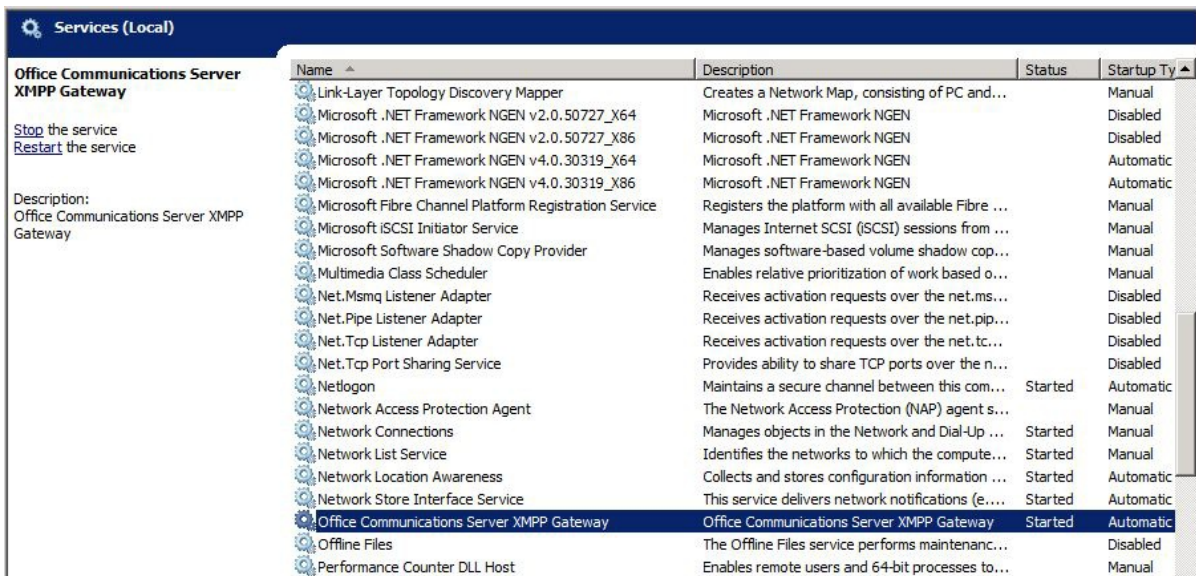


7. Select the Edge pool and identify whether a Next hop pool is configured below **Next hop selection**.



## Verify legacy XMPP federated partner Configuration

1. From the legacy XMPP server, navigate to the Administrative Tools\Services applet.
2. Verify that the Office Communications Server XMPP Gateway service is started.



# Phase 3: Deploy Skype for Business Server 2019 pilot pool

8/7/2019 • 2 minutes to read

This section covers the steps required to deploy a pilot pool of Skype for Business Server 2019. The deployment of Skype for Business Server 2019 requires using Topology Builder to define your topology and the components you want to deploy, preparing your environment for deployment of the Skype for Business Server 2019 components, publishing your topology design on the first Front End Server, and then installing and configuring Skype for Business Server 2019 software for the components for your deployment. When completed, your Skype for Business Server 2019 pilot pool deployment will coexist with an existing legacy pool.

## In this section

- [Prepare Active Directory for Skype for Business Server](#)
- [Download topology from existing deployment](#)
- [Deploy Skype for Business Server 2019 pilot pool](#)
- [Verify pilot pool coexistence with legacy pool](#)
- [Connect pilot pool to legacy Edge Servers](#)
- [Configure XMPP gateway access policies and certificates](#)

# Prepare Active Directory for Skype for Business Server

8/7/2019 • 2 minutes to read

Before deploying Skype for Business Server 2019 in a coexistence state, you must perform some additional Active Directory tasks to configure the schema, forest, and domain for Skype for Business Server 2019. The schema extensions add the Active Directory classes and attributes that are required by Skype for Business Server 2019.

## To prepare Active Directory for Skype for Business Server 2019

1. On the Skype for Business Server 2019 Front End Server, run Skype for Business Server 2019 Setup.
2. Select **Prepare Active Directory**.
3. Complete steps 1 through 5 in the wizard.

# Download topology from existing deployment

8/7/2019 • 2 minutes to read

When creating a Skype for Business Server 2019 pool, you will use the Central Management Store that is associated with the legacy installation. When you start Topology Builder on first use and subsequent edit sessions, you are prompted for the location where you want Topology Builder to load the current configuration document. Because you already have a topology defined and have established the Central Management store, you should choose to download a topology from an existing deployment. Topology Builder will read the database and retrieve the current definition.

## To download a topology from an existing deployment

1. Open the Skype for Business Server Deployment Wizard.
2. From the **Skype for Business Server 2019 - Deployment Wizard** page, click **Install Administrative Tools**.
3. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Topology Builder**.
4. Select **Download Topology from existing deployment**.
5. Choose a file name, and save the topology with the default .tbxml file type.
6. Expand the Skype for Business Server node to reveal the various server roles in the deployment.



# Deploy Skype for Business Server 2019 pilot pool

8/7/2019 • 3 minutes to read

One of the first steps required for migration to Skype for Business Server 2019 is to deploy a pilot pool. The pilot pool is where you test coexistence of Skype for Business Server 2019 with your legacy deployment. Coexistence is a temporary state that lasts until you have moved all users and pools to Skype for Business Server 2019.

When you deploy a pilot pool, you use the Define New Front End Pool wizard. You should deploy the same features and workloads in your Skype for Business Server 2019 pilot pool that you have in your legacy pool. If you deployed Archiving Server, Monitoring Server, or System Center Operations Manager for archiving or monitoring your legacy environment, and you want to continue archiving or monitoring throughout the migration, you need to also deploy these features in your pilot environment. The version you deployed to archive or monitor your legacy environment will not capture data in your Skype for Business Server 2019 environment.

## NOTE

The following procedure discusses features and settings you should consider as part of your overall pilot pool deployment process. This section only highlights key points you should consider as part of your pilot pool deployment.

## To deploy a Skype for Business Server 2019 pilot pool

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Expand the tree until you reach **Skype for Business Server 2019 > Enterprise Edition Front End pools**.
3. Right-click **Enterprise Edition Front End pools** and select **New Front End Pool**.
4. Enter the pool fully qualified domain name (FQDN). When you define your pilot pool, you can choose to deploy an Enterprise Edition Front End pool or a Standard Edition server. Skype for Business Server 2019 does not require that your pilot pool features match what was deployed in your legacy pool.

### Caution

The pool or server FQDN that you define for the pilot pool must be unique. It cannot match the name of the currently deployed legacy pool or any other servers currently deployed.

5. On the **Select features** page, select the check boxes for the features that you want on this Front End pool. For example, if you are deploying only instant messaging (IM) and presence features, you would select the Conferencing check box to allow multiparty IM, but you would not select the Dial-in (PSTN) conferencing, Enterprise Voice, or Call Admission Control check boxes, because they represent voice, video, and collaborative conferencing features.
6. On the **Select collocated server roles** page, we recommend that you choose to collocate the Mediation Server in Skype for Business Server 2019. When merging a legacy topology with Skype for Business Server 2019, we require that you first collocate the legacy Mediation Server. After merging the topologies and configuring the Skype for Business Server 2019 Mediation Server, you can decide whether to keep the collocated Mediation Server, or change it to a stand-alone server when you move the Mediation Server role to Skype for Business Server 2019 later in the deployment process.
7. On the **Associate server roles with this Front End pool** page, during pilot pool deployment, *do not* choose the **Enable an Edge pool to be used by the media component of this Front End pool** option. This is a feature you will enable and bring online in a later phase of migration. Keep this setting cleared for now.

8. On the **Select an Office Web Apps Server** page, click **New**, and specify the FQDN of the application server.
9. On the **Define the Archiving SQL Server store** page, when defining the SQL Server store for both Skype for Business Server Archiving and Monitoring, select the SQL Server instance created earlier for Skype for Business Server 2019.
10. To publish your topology, right-click the **Skype for Business Server** node, and then click **Publish Topology**.
11. When the publish process has completed, click **Finish**.
12. Before moving to the next section called "Verify pilot pool coexistence with legacy pool" you need to install the Skype for Business Server new Front End pilot pool we just defined in the published topology, follow the procedures outlined here [Install Skype for Business Server on servers in the topology](#)
13. Once previous step is complete, move to the next section to Verify pilot pool coexistence with legacy pool.

# Verify pilot pool coexistence with legacy pool

8/7/2019 • 2 minutes to read

## In this article

[Verify that Skype for Business Server 2019 services have started](#)

[Open the Skype for Business Server 2019 Control Panel](#)

[Don't attempt to open the topology in the legacy Topology Builder](#)

After you deploy the pilot pool, you need to verify the coexistence of the two pools by using the administrative tools to view the pool information. For the Skype for Business Server 2019 pools and legacy pools, you must use the Skype for Business Server 2019 Control Panel and Topology Builder tools.

## Verify that Skype for Business Server 2019 services have started

1. From the Skype for Business Server 2019 Front End Server, navigate to the Administrative Tools\Services applet.
2. Verify that the following services are running on the Front End Server:
  - Centralized Logging Service Agent
  - Application Sharing
  - Audio Test Service
  - Audio/Video Conferencing
  - Call Park
  - Conferencing Announcement
  - Conferencing Attendant
  - Front-End
  - IM Conferencing
  - Mediation
  - Replica Replicator Agent
  - Response Group
  - Web Conferencing
  - XMPP Translating Gateway

## Open the Skype for Business Server 2019 Control Panel

From the Front End Server in your Skype for Business Server 2019 deployment, open the Skype for Business Server 2019 Control Panel and select the legacy pool. Repeat the procedure to open the Skype for Business Server 2019 pool.

### IMPORTANT

On Skype for Business Server 2019, you must upgrade Silverlight to Silverlight version 5 prior to using the Skype for Business Server Control Panel.

This topology now includes legacy and Skype for Business Server 2019 server roles.

## Don't attempt to open the topology in the legacy Topology Builder

The topology can only be viewed using Skype for Business Server 2019 Topology Builder. The Skype for Business Server 2019 Topology Builder must be used to create pools for both Skype for Business Server 2019 and the legacy install.

# Connect pilot pool to legacy Edge Servers

8/7/2019 • 2 minutes to read

After deploying Skype for Business Server 2019, you need to configure a federation route for your site. In order to use the federated route that is being used by the legacy installation, Skype for Business Server 2019 must be configured to use this route.

To enable the Skype for Business Server 2019 site to use the Director and Edge Server of the legacy deployment, use Topology Builder to associate the legacy Edge pool.

## To associate the legacy Edge pool by using Topology Builder

1. Open Topology Builder.
2. Select your site, which is directly below the **Skype for Business Server** node.
3. On the **Actions** menu, click **Edit Properties**.
4. In the left pane, select **Federation route**.
5. Under **Site federation route assignment**, select **Enable SIP federation**, and then select the legacy Director, or the legacy Edge Server if no Director is listed.
6. Click **OK** to close the **Edit Properties** page.
7. In Topology Builder, under the Skype for Business Server 2019 node, navigate to the **Standard Edition server** or **Enterprise Edition Front End pools**, right-click the pool, and then click **Edit Properties**.
8. Under **Associations**, select the check box next to **Associate Edge pool (for media components)**.
9. From the list, select the legacy Edge Server.
10. Click **OK** to close the **Edit Properties** page.
11. In **Topology Builder**, select the top-most node, **Skype for Business Server**.
12. From the **Action** menu, click **Publish Topology**, and then click **Next**.
13. When the **Publishing wizard** completes, click **Finish**.

# Configure XMPP gateway access policies and certificates

8/7/2019 • 2 minutes to read

XMPP federation defines an external deployment based on the eXtensible Messaging and Presence Protocol (XMPP). An XMPP configuration allows users access to XMPP domain users by:

- IM and Presence - person to person only
- Creation of XMPP federated contacts in the Skype for Business client

When you configure policies for support of XMPP federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers, or SIP federated domains. You configure an XMPP federated partner for each XMPP federated domain that you want to allow your users to add contacts and communicate with. Once the policies are in place, you need to configure the XMPP Gateway certificates.

## NOTE

XMPP functionality is deprecated in Skype for Business Server 2019, but can be continued in a legacy server in coexistence with Skype for Business Server 2019. Make sure you have already deployed the legacy server (Skype for Business Server 2015 / Lync Server 2013) XMPP Gateway, and configured the access policies to enable users for legacy XMPP Gateway. For details, see [Migrating XMPP Federation](#).

## Configure an External Access Policy to Enable Users for legacy XMPP Gateway

1. Open the legacy Skype for Business Server Control Panel.
2. In the left navigation bar, click **Federation and External Access**, and then click **External Access Policy**.
3. Click **New**, and then click **User policy**.
4. Enter a name for the external access user policy.
5. Provide a description for external access user policy.
6. Select **Enable communications with federated users**.
7. Select **Enable communications with XMPP federated users**.
8. Click **Commit** to save your changes to the site or user policy.

# Phase 4: Move test users to the pilot pool

8/7/2019 • 2 minutes to read

You can move a single user or groups of users to your new Microsoft Skype for Business Server 2019 deployment using the following two methods: Skype for Business Server Control Panel and Skype for Business Server Management Shell. The topics in this section describe tasks you must complete during pilot deployment, as well as prior to moving your deployment of Skype for Business Server 2019 from a pilot deployment to a production-level deployment.

## In this section

- [View current users in legacy pool](#)
- [Verify user replication has completed](#)
- [Move a single user to the pilot pool](#)
- [Move multiple users to the pilot pool](#)

# View current users in legacy pool

8/7/2019 • 2 minutes to read

Before learning the various ways you can move users between pools, we must first determine which users exist in the legacy pool. The **Registrar pool** column identifies users who are configured for the legacy pool. These are the test users we will move to the Skype for Business Server 2019 pool.

## To see the list of users in the legacy pool

1. Log on to the legacy Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open **Skype for Business Server Control Panel**.
3. Click **Users**, click **Search**, and then click **Find**.



# Verify user replication has completed

8/7/2019 • 2 minutes to read

When running the **Move-CsUser** cmdlet, you may experience a failure if user information between Active Directory Domain Services (AD DS) and the Skype for Business Server 2019 databases are out of sync because the initial replication is incomplete. The time it takes for the successful completion of the Skype for Business Server 2019 User Replicator service's initial synchronization depends on the number of domain controllers that are hosted in the Active Directory forest that hosts the Skype for Business Server 2019 pool. The Skype for Business Server 2019 User Replicator service initial synchronization process occurs when the Skype for Business Server 2019 Front End Server is started for the first time. After that, the synchronization is based on the User Replicator interval. Complete the following steps to verify that user replication has completed before running the **Move-CsUser** cmdlet.

## To verify that user replication has completed

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Click the **Start** menu, and then click **Run**.
3. Enter **eventvwr.exe**, and then click **OK**.
4. In Event Viewer, click **Applications and Services logs** to expand it, and then select Skype for Business Server.
5. In the **Actions** pane, click **Filter Current Log**.
6. From the **Event sources** list, click **LS User Replicator**.
7. In **<All Event IDs>**, enter **30024**, and then click **OK**.
8. In the filtered events list, on the **General** tab, look for an entry that states that user replication has completed successfully.

# Move a single user to the pilot pool

8/7/2019 • 2 minutes to read

You can move a user from your legacy pool to your Skype for Business Server 2019 pilot pool using Skype for Business Server 2019 Control Panel or Skype for Business Server 2019 Management Shell. In the example below, in the **Registrar pool** column, **pool01.contoso.net** is the legacy pool, and all six of these users are connected to this pool. Use the following procedures to move a user to your Skype for Business Server 2019 pool using Skype for Business Server 2019 Control Panel and Skype for Business Server Management Shell.

## To move a user by using the Skype for Business Server 2019 Control Panel

1. Log on to the Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open **Skype for Business Server Control Panel**.
3. Click **Users**, click **Search**, and then click **Find**.
4. Select a user that you want to move to the Skype for Business Server 2019 pool. In this example, we will move user Sara Davis.
5. On the **Action** menu, select **Move selected users to pool**.
6. From the drop-down list, select the Skype for Business Server 2019 pool.
7. Click **Action**, and then click **Move selected users to pool**. Click **OK**.
8. Verify that the **Registrar pool** column for the user now contains the Skype for Business Server 2019 pool, which indicates that the user has been successfully moved.

## To move a user by using the Skype for Business Server 2019 Management Shell

1. Open the Skype for Business Server Management Shell.
2. At the command line, type the following:

```
Move-CsUser -Identity "David Pelton" -Target "pool02.contoso.net"
```

3. Next, at the command line, type the following:

```
Get-CsUser -Identity "David Pelton"
```

4. The **RegistrarPool** identity now points to the Skype for Business Server 2019 pool. The presence of this identity confirms that the user has been successfully moved.

### NOTE

For details about the **Get-CsUser** cmdlet, run: **Get-Help Get-CsUser -Detailed**

# Move multiple users to the pilot pool

8/7/2019 • 2 minutes to read

You can move multiple users from your legacy pool to your Skype for Business Server 2019 pilot pool using Skype for Business Server 2019 Control Panel or Skype for Business Server 2019 Management Shell.

## In this article

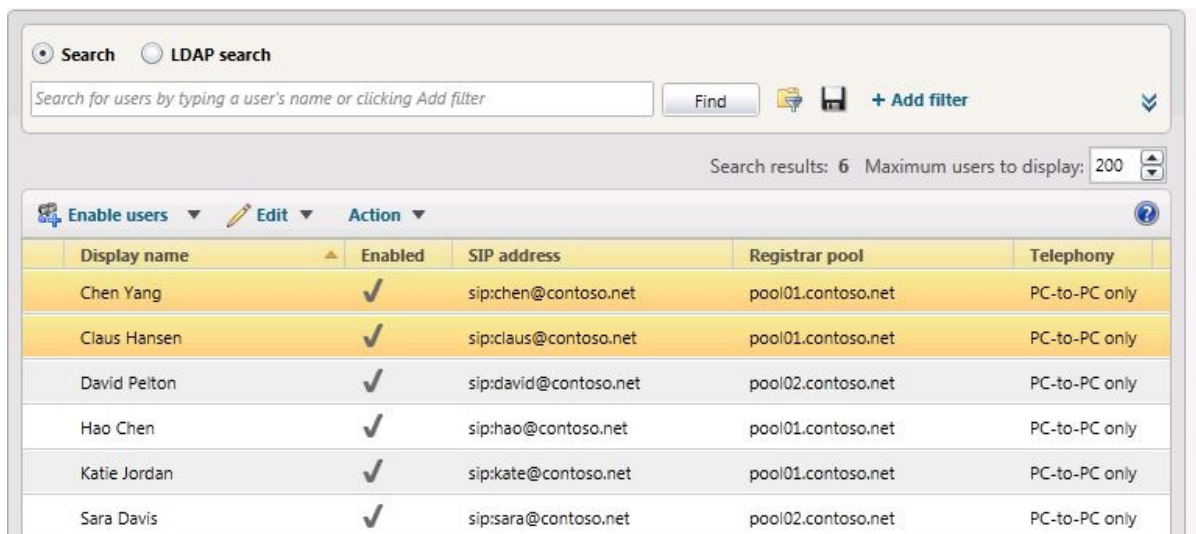
[To move multiple users by using the Skype for Business Server 2019 Control Panel](#)

[To move multiple users by using the Skype for Business Server 2019 Management Shell](#)

[To move all users at the same time by using the Skype for Business Server 2019 Management Shell](#)

## To move multiple users by using the Skype for Business Server 2019 Control Panel

1. Open Skype for Business Server Control Panel.
2. Click **Users**, click **Search**, and then click **Find**.
3. Select two users that you want to move to the Skype for Business Server 2019 pool. In this example, we will move users Chen Yang and Claus Hansen.



The screenshot shows the 'Search' interface in the Skype for Business Server 2019 Control Panel. The search results are displayed in a table with the following columns: Display name, Enabled, SIP address, Registrar pool, and Telephony. The first two rows, 'Chen Yang' and 'Claus Hansen', are highlighted in yellow, indicating they are selected. The 'Enabled' column for all users shows a checkmark. The 'Registrar pool' for Chen Yang and Claus Hansen is 'pool01.contoso.net', while for the other users, it is either 'pool01.contoso.net' or 'pool02.contoso.net'. The 'Telephony' column for all users is 'PC-to-PC only'.

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool01.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool01.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool02.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool01.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool01.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool02.contoso.net	PC-to-PC only

4. From the **Action** menu, select **Move selected users to pool**.
5. From the drop-down list, select the Skype for Business Server 2019 pool.
6. Click **Action**, and then click **Move selected users to pool**. Click **OK**.

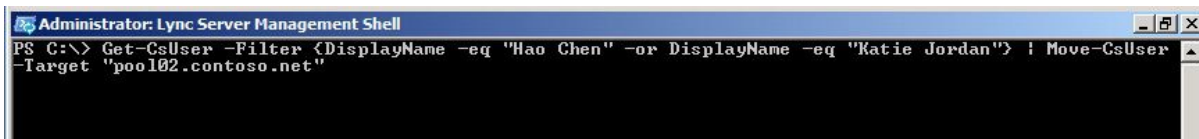


7. Verify that the **Registrar pool** column for the users now contains the Skype for Business Server 2019 pool, which indicates that the users have been successfully moved.

## To move multiple users by using the Skype for Business Server 2019 Management Shell

1. Open the Skype for Business Server 2019 Management Shell.
2. At the command line, type the following and replace **User1** and **User2** with specific user names you want to move, and replace **pool\_FQDN** with the name of the destination pool. In this example we will move users Hao Chen and Katie Jordan.

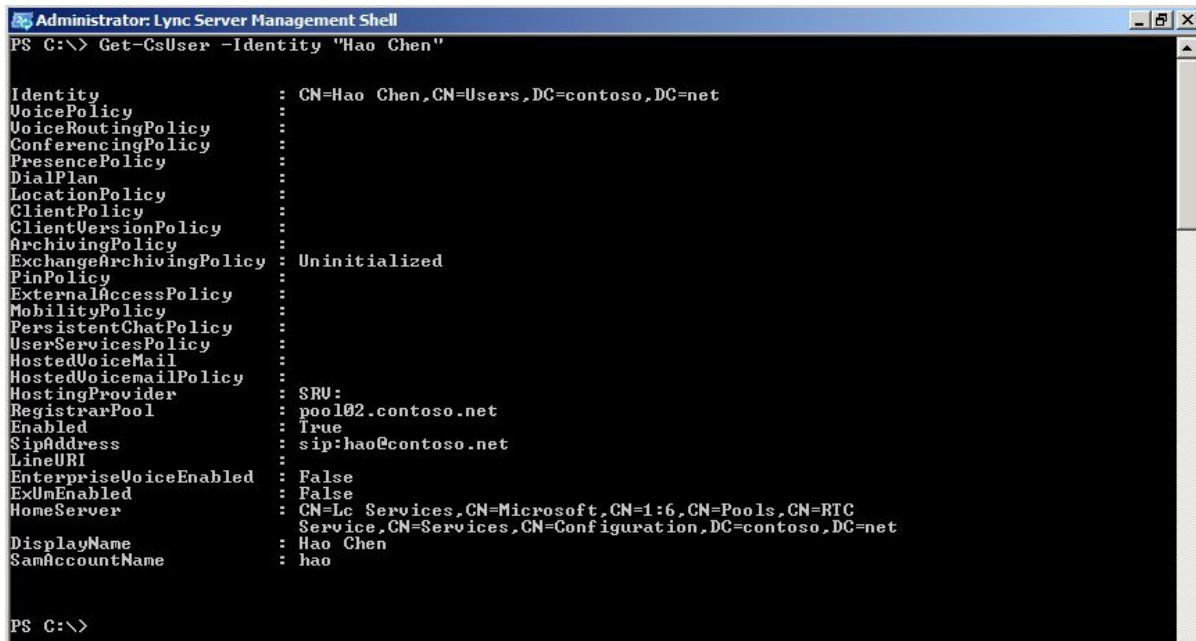
```
Get-CsUser -Filter {DisplayName -eq "User1" -or DisplayName - eq "User2"} | Move-CsUser -Target "pool_FQDN"
```



3. At the command line, type the following:

```
Get-CsUser -Identity "User1"
```

4. The **Registrar Pool** identity should now point to the pool you specified as **pool\_FQDN** in the previous step. The presence of this identity confirms that the user has been successfully moved. Repeat step to verify that **User2** has been moved.



```
Administrator: Lync Server Management Shell
PS C:\> Get-CsUser -Identity "Hao Chen"

Identity           : CN=Hao Chen,CN=Users,DC=contoso,DC=net
VoicePolicy        :
VoiceRoutingPolicy :
ConferencingPolicy :
PresencePolicy     :
DialPlan           :
LocationPolicy     :
ClientPolicy       :
ClientVersionPolicy :
ArchivingPolicy    :
ExchangeArchivingPolicy : Uninitialized
PinPolicy          :
ExternalAccessPolicy :
MobilityPolicy     :
PersistentChatPolicy :
UserServicesPolicy :
HostedVoiceMail    :
HostedVoicemailPolicy :
HostingProvider    : SRU:
RegistrarPool     : pool02.contoso.net
Enabled            : True
SipAddress         : sip:hao@contoso.net
LineURI            :
EnterpriseVoiceEnabled : False
ExUnEnabled        : False
HomeServer         : CN=Lc Services,CN=Microsoft,CN=1:6,CN=Pools,CN=RTC
                   : Service,CN=Services,CN=Configuration,DC=contoso,DC=net
DisplayName        : Hao Chen
SamAccountName     : hao

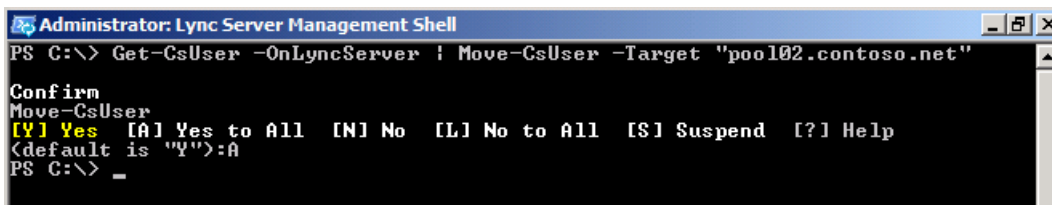
PS C:\>
```

## To move all users at the same time by using the Skype for Business Server 2019 Management Shell

In this example, all users have been returned to the legacy pool (pool01.contoso.net). Using the Skype for Business Server 2019 Management Shell, we will move all users at the same time to the Skype for Business Server 2019 pool (pool02.contoso.net).

1. Open the Skype for Business Server 2019 Management Shell.
2. At the command line, type the following:

```
Get-CsUser -OnLyncServer | Move-CsUser -Target "pool_FQDN"
```



```
Administrator: Lync Server Management Shell
PS C:\> Get-CsUser -OnLyncServer | Move-CsUser -Target "pool02.contoso.net"

Confirm
Move-CsUser
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):A
PS C:\> _
```

3. Run **Get-CsUser** for one of the pilot users.

```
Get-CsUser -Identity "Hao Chen"
```

4. The **Registrar Pool** identity for each user now points to the pool you specified as **pool\_FQDN** in the previous step. The presence of this identity confirms that the user has been successfully moved.
5. Additionally, we can view the list of users in the Skype for Business Server 2019 Control Panel and verify that the Registrar Pool value now points to the Skype for Business Server 2019 pool.

Search  LDAP search

Search for users by typing a user's name or clicking Add filter

Find



+ Add filter



Search results: 6 Maximum users to display: 200

Enable users Edit Action



Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool02.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool02.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool02.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool02.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool02.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool02.contoso.net	PC-to-PC only

# Phase 5: Add Skype for Business Server 2019 Edge Server to pilot pool

8/7/2019 • 2 minutes to read

The topics in this section explain how to add a Skype for Business Server 2019 Edge Server to the pilot pool deployment. The topics provide configuration and verification guidance when running the Deploy New Edge pool wizard.

## In this section

- [Deploy pilot Edge Server](#)
- [Verify configuration settings](#)

# Deploy pilot Edge Server

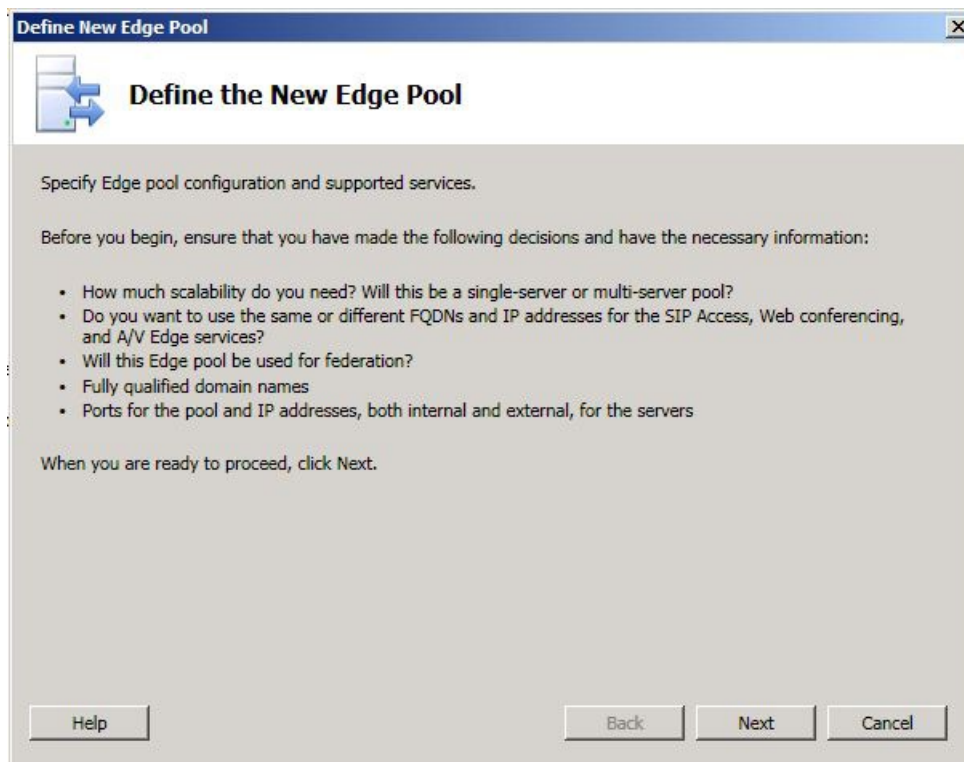
8/7/2019 • 2 minutes to read

This topic highlights configuration settings you should be aware of before deploying your Skype for Business Server 2019 Edge Server. The deployment and configuration processes for Skype for Business Server 2019 are very similar to Skype for Business Server 2015. This section only highlights key points you should consider as part of your pilot pool deployment.

As you navigate through the **Define New Edge Pool** wizard, review the key configuration settings shown in the following steps. Note that only a few pages of the **Define New Edge Pool** wizard are shown.

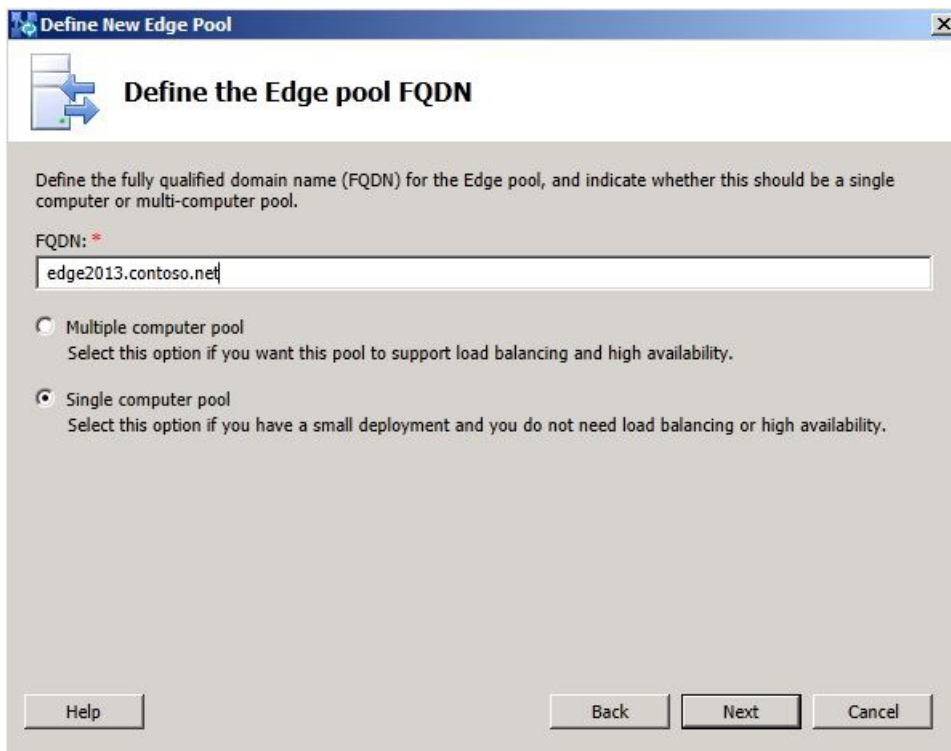
## To define an Edge Pool

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Navigate to the Skype for Business Server 2019 node. Right-click **Edge pools**, and click **New Edge pool**.

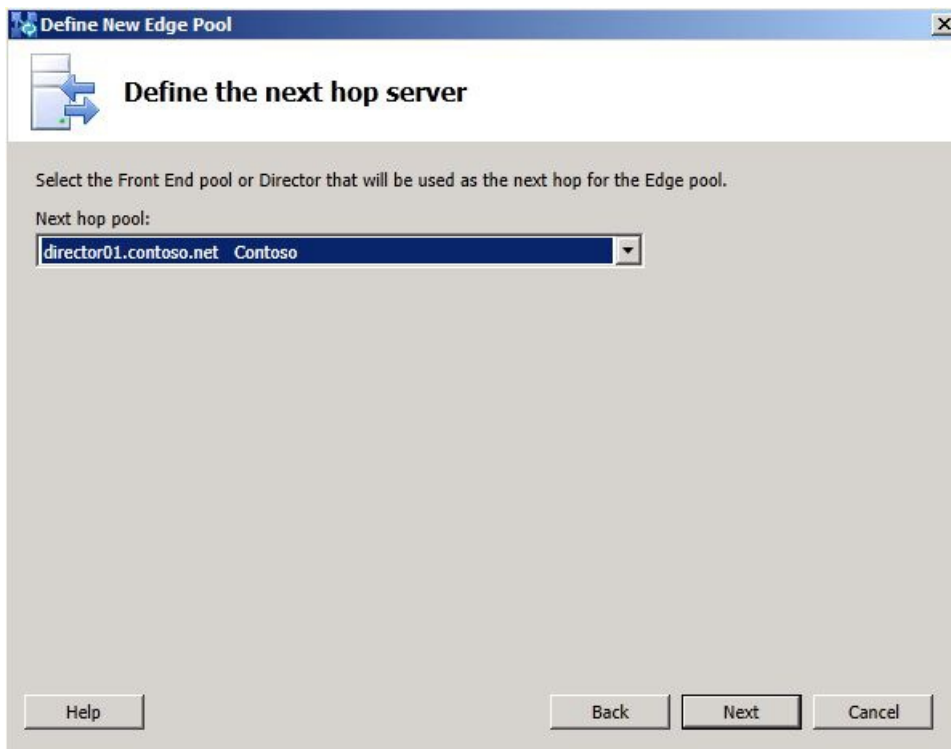


3. An Edge pool can be a **Multiple computer pool** or **Single computer pool**.

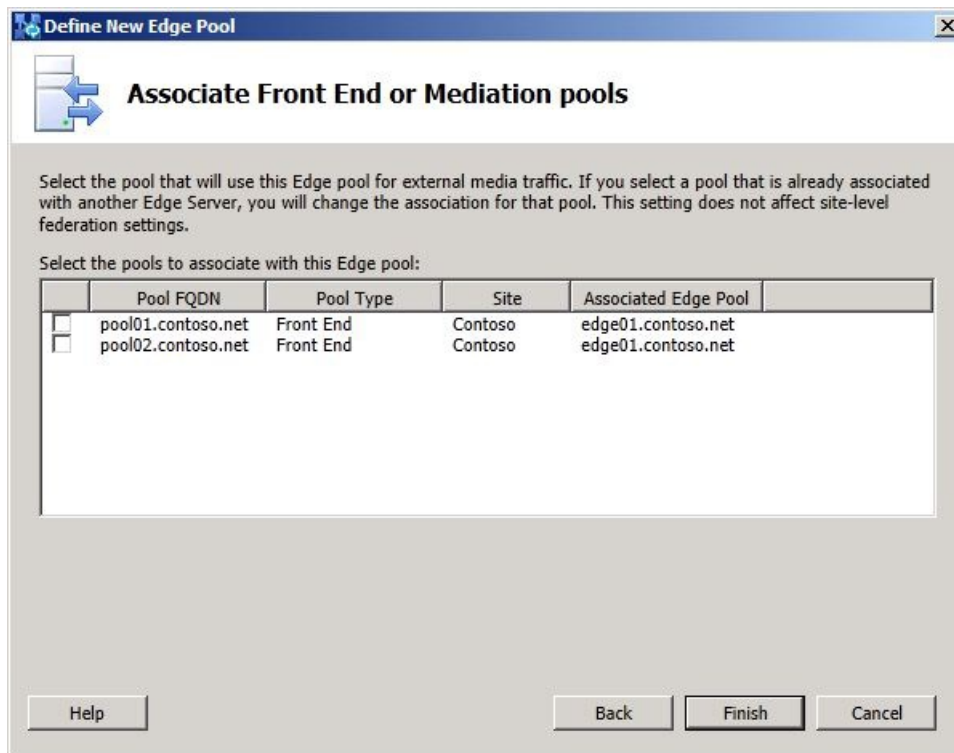




4. On the **Select features** page, do not enable federation or XMPP federation. Federation and XMPP federation are both currently routed through the legacy Edge Server. These features will be configured in a later phase of migration.
5. Continue completing the following wizard pages: **External FQDNs**, **Define the internal IP address**, and **Define the external IP address**.
6. On the **Define the next hop server** page, select the Director for the next hop of the legacy Edge pool.



7. On the **Associate Front End or Mediation pools** page, do not associate a pool with this Edge pool at this time. External media traffic is currently routed through the legacy Edge Server. This setting will be configured in a later phase of migration.



8. Click **Finish**, and then **Publish** the topology.
9. Follow the steps in the Deployment documentation to install the files on the new Edge Server, configure certificates, and start the services.

It's very important that you follow the guidelines in the topics in the Deployment documentation. This section merely provided some guidance on configuration settings when installing these server roles.

You should now have a legacy Edge Server deployed in parallel with a Skype for Business Server 2019 Edge server deployment. Verify that both deployments are running properly, services are started, and you can administer each deployment prior to moving to the next phase.

# Verify configuration settings

8/7/2019 • 2 minutes to read

You can validate the replication of configuration information to the Edge server by running the Skype for Business Server 2019 **Get-CsManagementStoreReplicationStatus** cmdlet on the internal computer on which the Central Management store is located, or on any domain-joined computer on which Skype for Business Server 2019 Core Components (OcsCore.msi) is installed.

Initial results may indicate the status as "False" instead of "True" for replication. If so, run the **Invoke-CsManagementStoreReplication** cmdlet and allow time for the replication to complete before running the **Get-CsManagementStoreReplicationStatus** again.

# Phase 6: Move from pilot deployment into production

8/7/2019 • 2 minutes to read

The topics in this section describe tasks you must complete before moving your deployment of Skype for Business Server 2019 from a pilot deployment to a production-level deployment.

## In this section

- [Configure federation routes and media traffic](#)
- [Verify federation and remote access for external users](#)
- [Change simple URLs after migration](#)
- [Move remaining users to Skype for Business Server 2019](#)

# Configure federation routes and media traffic

8/7/2019 • 7 minutes to read

Federation is a trust relationship between two or more SIP domains that permits users in separate organizations to communicate across network boundaries. After you migrate to your pilot pool, you need to transition from the federation route of your previous version's Edge Servers to the federation route of your Skype for Business Server 2019 Edge Servers.

Use the following procedures to transition the federation route and the media traffic route from your previous version's Edge Server and Director to your Skype for Business Server 2019 Edge Server, for a single-site deployment.

## IMPORTANT

Changing the federation route and media traffic route requires that you schedule maintenance downtime for the Skype for Business Server 2019 and previous version Edge Servers. This entire transition process also means that federated access will be unavailable for the duration of the outage. You should schedule the downtime for a time when you expect minimal user activity. You should also provide sufficient notification to your end users. Plan accordingly for this outage and set appropriate expectations within your organization.

## IMPORTANT

If your legacy Edge Server is configured to use the same FQDN for the Access Edge service, Web Conferencing Edge service, and the A/V Edge service, the procedures in this section are not supported. If the legacy Edge services are configured to use the same FQDN, you must first migrate all your users, then decommission the previous versions Edge Server before enabling federation on the Skype for Business Server 2019 Edge Server.

## IMPORTANT

If your XMPP federation is routed through a Skype for Business Server 2019 Edge Server, users on the previous version will not be able to communicate with the XMPP federated partner until all users have been moved to Skype for Business Server 2019, XMPP policies and certificates have been configured, the XMPP federated partner has been configured on Skype for Business Server 2019, and, lastly, the DNS entries have been updated.

## To remove the legacy federation association from Skype for Business Server 2019 sites

1. On the Skype for Business Server 2019 Front End server, open the existing topology in Topology Builder.
2. In the left pane, navigate to the site node, which is located directly below **Skype for Business Server**.
3. Right-click the site, and then click **Edit Properties**.
4. In the left pane, select **Federation route**.
5. Under **Site federation route assignment**, clear the **Enable SIP federation** check box to disable the federation route through the legacy environment.
6. Click **OK** to close the Edit Properties page.

7. From **Topology Builder**, select the top node **Skype for Business Server**.
8. From the **Action** menu, click **Publish Topology**.
9. Click **Next** to complete the publishing process, and then click **Finish** when the publishing process has completed.

## To configure the legacy Edge Server as a non-federating Edge Server

1. In the left pane, navigate to the legacy install node and then to the **Edge pools** node.
2. Right-click the Edge server, and then click **Edit Properties**.
3. Select **General** in the left pane.
4. Clear the **Enable federation for this Edge pool (port 5061)** check box and select **OK** to close the page.
5. From the **Action** menu, select **Publish Topology**, and then click **Next**.
6. When the **Publishing wizard** completes, click **Finish** to close the wizard.
7. Verify that federation for the legacy Edge server is disabled in Topology Builder.

## To configure certificates on the legacy Edge Server

1. Export the external Access Proxy certificate, with the private key, from the legacy Edge Server.
2. On the Skype for Business Server 2019 Edge Server, and import the Access Proxy external certificate from the previous step.
3. Assign the Access Proxy external certificate to the Skype for Business Server 2019 external interface of the Edge Server.
4. The internal interface certificate of the Skype for Business Server 2019 Edge Server should be requested from a trusted CA and assigned.

## To change the previous version's federation route to use Skype for Business Server 2019 Edge Server

1. From Topology Builder, in the left pane, navigate to the **Skype for Business Server 2019** node and then to the **Edge pools** node.
2. Right-click the Edge server, and then click **Edit Properties**.
3. Select **General** in the left pane.
4. Select the check box for **Enable federation for this Edge pool (port 5061)**, and then click **OK** to close the page.
5. From the **Action** menu, select **Publish Topology**, and then click **Next**.
6. When the **Publishing wizard** completes, click **Finish** to close the wizard.
7. Verify that **Federation (port 5061)** is set to **Enabled** in Topology Builder.

## To update Skype for Business Server 2019 Edge Server federation next hop

1. From Topology Builder, in the left pane, navigate to the **Skype for Business Server 2019** node and then to the **Edge pools** node.

2. Expand the node, right-click the Edge Server listed, and then click **Edit Properties**.
3. On the **General** page, under **Next hop selection**, select from the drop-down list the Skype for Business Server 2019 pool.
4. Click **OK** to close the Edit Properties page.
5. From **Topology Builder**, select the top node **Skype for Business Server**.
6. From the **Action** menu, click **Publish Topology** and complete the wizard.

## To configure Skype for Business Server 2019 Edge Server outbound media path

1. From Topology Builder, in the left pane, navigate to the **Skype for Business Server 2019** node and then to the pool below **Standard Edition Front End Servers** or **Enterprise Edition Front End pools**.
2. Right-click the pool, and then click **Edit Properties**.
3. In the **Associations** section, select the **Associate Edge pool (for media components)** check box.
4. From the drop-down box, select the Skype for Business Server 2019 Edge Server.
5. Click **OK** to close the **Edit Properties** page.

## To turn on Skype for Business Server 2019 Edge Server federation

1. From Topology Builder, in the left pane, navigate to the **Skype for Business Server 2019** node and then to the **Edge pools** node.
2. Expand the node, right-click the Edge Server listed, and then click **Edit Properties**.

### NOTE

Federation can only be enabled for a single Edge pool. If you have multiple Edge pools, select one to use as the federating Edge pool.

3. On the **General** page, verify that the **Enable federation for this Edge pool (Port 5061)** check box is selected.
4. Click **OK** to close the Edit Properties page.
5. Navigate to the site node.
6. Right-click the site, and then click **Edit Properties**.
7. In the left pane, click **Federation route**.
8. Under **Site federation route assignment**, select **Enable SIP federation**, and then from the list select the Skype for Business Server 2019 Edge Server listed.
9. Click **OK** to close the **Edit Properties** page.

For multi-site deployments, complete this procedure at each site.

## To publish Edge Server configuration changes

1. From **Topology Builder**, select the top node **Skype for Business Server**.

2. From the **Action** menu, select **Publish Topology** and complete the wizard.
3. Wait for Active Directory replication to occur to all pools in the deployment.

#### NOTE

You may see the following message: **Warning: The topology contains more than one Federated Edge Server. This can occur during migration to a more recent version of the product. In that case, only one Edge Server would be actively used for federation. Verify that the external DNS SRV record points to the correct Edge Server. If you want to deploy multiple federation Edge Server to be active concurrently (that is, not a migration scenario), verify that all federated partners are using Skype for Business Server. Verify that the external DNS SRV record lists all federation enabled Edge Servers.** This warning is expected and can be safely ignored.

## To configure Skype for Business Server 2019 Edge Server

1. Bring all of the Skype for Business Server 2019 Edge Servers online.
2. Update the external firewall routing rules or the hardware load balancer settings to send SIP traffic for external access (usually port 443) and federation (usually port 5061) to the Skype for Business Server 2019 Edge Server, instead of the legacy Edge Server.

#### NOTE

If you do not have a hardware load balancer, you need to update the DNS A record for federation to resolve to the new Skype for Business Server Access Edge server. To accomplish this with minimal disruption, reduce the TLL value for the external Skype for Business Server Access Edge FQDN so that when DNS is updated to point to the new Skype for Business Server Access Edge, federation and remote access will be updated quickly.

3. Stop the **Skype for Business Server Access Edge** from each Edge Server computer.
4. From each legacy Edge Server computer, open the **Services** applet from the **Administrative Tools**.
5. In the services list, find **Skype for Business Server Access Edge**.
6. Right-click the services name, and then select **Stop** to stop the service.
7. Set the Startup type to **Disabled**.
8. Click **OK** to close the **Properties** window.



# Verify federation and remote access for external users

8/7/2019 • 2 minutes to read

After transitioning the federation route to the Skype for Business Server 2019 Edge Server, you should perform some functional tests to verify that federation performs as expected. Tests for external user access should include each type of external user that your organization supports, including any or all of the following.

## **Test connectivity of external users and external access**

- Users from at least one federated domain, an internal user on Skype for Business Server 2019, and a user on the legacy install. Test instant messaging (IM), presence, audio/video (A/V), and desktop sharing.
- Users of each public IM service provider that your organization supports (and for which provisioning has been completed) communicating with a user on Skype for Business Server 2019 and a user on the legacy install.
- Verify that anonymous users are able to join conferences.
- A user hosted on the legacy install using remote user access (logging i nto Lync Server/Skype for Business from outside the intranet but without VPN) with a user on Skype for Business Server 2019, and a user on the legacy install. Test IM, presence, A/V, and desktop sharing.
- A user hosted on Skype for Business Server 2019 using remote user access (logging in to Skype for Business Server 2019 from outside the intranet but without VPN) with a user on Skype for Business Server 2019, and a user on the legacy install. Test IM, presence, A/V, and desktop sharing.

# Change simple URLs after migration

8/7/2019 • 2 minutes to read

Skype for Business Server supports three simple URLs:

- **Meet** is used as the base URL for all conferences in the site or organization. With the Meet simple URL, links to join meetings are easy to comprehend, and easy to communicate and distribute.
- **Dial-in** enables access to the Dial-in Conferencing Settings webpage. The Dial-in simple URL is included in all meeting invitations so that users who want to dial in to the meeting can access the necessary phone number and PIN information.
- **Admin** enables quick access to the Skype for Business Server Control Panel. The Admin simple URL is internal to your organization.

After migrating to Skype for Business Server, you must be aware of how the change impacts your DNS records and certificates for simple URLs. If the legacy Skype for Business Server Director remains in use in the topology, no changes to your simple URLs are required. If the Skype for Business Server Director is removed from the topology after migration, the simple URL DNS records must be updated to point to one of the Skype for Business Server pools. Whenever you change a simple URL name, however, you must run Enable-CsComputer on each Director and Front End Server to register the change.

## To update the Meet simple URL

1. In Topology Builder, right-click the top node **Skype for Business Server**, and then click **Edit Properties**.
2. Select **Simple URLs** in the left pane, then below **Meeting URLs**: select the Meet URL and then click **Edit URL**.
3. Update the URL to the value you want, and then click **OK** to save the edited URL.

## To update the Admin simple URL

1. In Topology Builder, right-click the top node **Skype for Business Server**, and then click **Edit Properties**.
2. Select **Simple URLs** in the left pane, then below **Administrative access URL** box, enter the simple URL you want for administrative access to Skype for Business Server Control Panel, and then click **OK**.

### TIP

We recommend using the simplest possible URL for the Admin URL. The simplest option is `https://admin.<domain>`.

## See also

[DNS requirements for simple URLs in Skype for Business Server](#)

# Move remaining users to Skype for Business Server 2019

8/7/2019 • 2 minutes to read

You can move users to the new Skype for Business Server 2019 deployment by using either Skype for Business Server Control Panel or Skype for Business Server Management Shell. You must meet some requirements to ensure a smooth transition to Skype for Business Server 2019. For details about prerequisites to completing the procedures in this topic, see [Configure clients for migration](#). For detailed steps about moving users, see [Phase 4: Move test users to the pilot pool](#).

## IMPORTANT

You cannot use the Active Directory Users and Computers snap-in or the legacy administrative tools to move users from your legacy environment to Skype for Business Server 2019.

When you move a user to a Skype for Business Server 2019 pool, the data for the user is moved to the back-end database that is associated with the new pool.

## IMPORTANT

This includes the active meetings created by the legacy user. For example, if a legacy user has configured a **my meeting** conference, that conference will still be available in the new Skype for Business Server 2019 pool after the user has been moved. The details to access that meeting will still be the same **conference URL and conference ID**. The only difference is that the conference is now hosted in the Skype for Business Server 2019 pool, and not in the legacy pool.

## NOTE

Homing users on Skype for Business Server 2019 does not require that you deploy upgraded clients at the same time. New functionality will be available to users only when they have upgraded to the new client software.

## Post migration task

1. After you move users, verify the conferencing policy that is assigned to them.
2. To ensure that meetings organized by users homed on Skype for Business Server 2019 work seamlessly with federated users who are homed on legacy install, the conferencing policy assigned to the migrated users should allow anonymous participants.
3. Conferencing policies that allow anonymous participants have **Allow participants to invite anonymous users** selected in Skype for Business Server 2019 Control Panel and have **AllowAnonymousParticipantsInMeetings** set to **True** in the output from the **Get-CsConferencingPolicy** cmdlet in the Skype for Business Server Management Shell.

# Phase 7: Complete post-migration tasks

8/7/2019 • 2 minutes to read

The topics in this section describe tasks that you will need to perform after you have completed your migration to Skype for Business Server 2019.

## In this section

- [Migrate existing meetings and meeting content](#)
- [Migrate dial-in access numbers](#)
- [Migrate Call Park application settings](#)
- [Migrate response groups](#)
- [Migrate Address Book](#)
- [Configure the meeting join page](#)
- [Remove legacy Archiving and Monitoring servers](#)
- [Configure trusted application servers](#)
- [Deploy Skype for Business Server 2019 clients](#)
- [Connect a Survivable Branch Appliance](#)
- [Configure SCOM monitoring](#)
- [Migrate Common Area Phones](#)
- [Migrate analog devices](#)

# Migrate existing meetings and meeting content

8/7/2019 • 2 minutes to read

When a user account is moved to a Skype for Business Server 2019 server, the following information is moved with that user account:

- **Meetings already scheduled by the user.** This includes moving the conferencing directories and conferencing data.
- **User's personal identification number (PIN).** The user's current PIN continues to work until it expires or the user requests a new PIN.

The following user account information does not move to the new server.

- **Meeting content.** In order to move the content shared during a meeting, such as PowerPoint, Whiteboard, attachments, or poll data, use the **-MoveConferenceData** parameter as part of the **Move-CsUser** cmdlet.

# Migrate dial-in access numbers

8/7/2019 • 2 minutes to read

Migrating dial-in access numbers to Skype for Business Server 2019 requires running the **Move-CsApplicationEndpoint** cmdlet to migrate the contact objects. During the legacy install and Skype for Business Server 2019 coexistence period, dial-in access numbers that you created in Skype for Business Server 2019 behave similarly to the dial-in access numbers that you create in the legacy install, as described in this section.

Dial-in access numbers that you created in the legacy install but moved to Skype for Business Server 2019, or that you created in Skype for Business Server 2019 before, during, or after migration, have the following characteristics:

- Do not appear on Office Communications Server 2007 R2 meeting invitations and the dial-in access number page.
- Appear on the legacy install meeting invitations and the dial-in access number page.
- Appear on Skype for Business Server 2019 meeting invitations and the dial-in access number page.
- Cannot be viewed or modified in the Office Communications Server 2007 R2 administrative tool.
- Can be viewed and modified in the legacy install Control Panel and in the legacy install Management Shell.
- Can be viewed and modified in the Skype for Business Server 2019 Control Panel and in Skype for Business Server 2019 Management Shell.
- Can be re-sequenced within the region by using the `Set-CsDialinConferencingAccessNumber` cmdlet with the `Priority` parameter.

You must finish migrating dial-in access numbers that point to the legacy install pool before you decommission the legacy install pool. If you do not complete dial-in access number migration as described in the following procedure, incoming calls to the access numbers will fail.

## IMPORTANT

You must perform this procedure prior to decommissioning the legacy install pool.

## NOTE

We recommend that you move dial-in access numbers when network usage is low, in case there is a short period of service outage.

## To identify and move dial-in access numbers

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Management Shell**.
2. To move each dial-in access number to a pool hosted on Skype for Business Server 2019, from the command line run:

```
Move-CsApplicationEndpoint -Identity <SIP URI of the access number to be moved> -Target <FQDN of the pool to which the access number is moving>
```

3. Open Skype for Business Server Control Panel.
4. In the left navigation bar, click **Conferencing**.
5. Click the **Dial-in Access Number** tab.
6. Verify that no dial-in access numbers remain for the legacy install pool from which you are migrating.

#### NOTE

When all dial-in access numbers point to the Skype for Business Server 2019 pool, you can then decommission the legacy install pool.

## Verify the dial-in access number migration using Skype for Business Server Control Panel

1. From a user account that is assigned to the **CsUserAdministrator** role or the **CsAdministrator** role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**.
4. Click the **Dial-in Access Number** tab.
5. Verify that all the dial-in access numbers are migrated to the pool hosted on Skype for Business Server 2019.

## Verify the dial-in access number migration using Skype for Business Server Management Shell

1. Open Skype for Business Server Management Shell.
2. To return all the dial-in conferencing access numbers migrated, from the command line run:

```
Get-CsDialInConferencingAccessNumber -Filter {Pool -eq "<FQDN of the pool to which the access number is moved>"}
```

3. Verify that all the dial-in access numbers are migrated to the pool hosted on Skype for Business Server 2019.

# Migrate Call Park application settings

8/7/2019 • 3 minutes to read

The migration of the Call Park application includes provisioning the Skype for Business Server 2019 pool with any custom music-on-hold files that have been uploaded in the legacy install, restoring the service-level settings and re-targeting all Call Park orbits to the Skype for Business Server 2019 pool. If customized music-on-hold files have been configured in the pool, these files need to be copied to the new Skype for Business Server 2019 pool. Additionally, it is recommended that you back up any Call Park customized music-on-hold files to another destination to keep a separate backup copy of any customized music-on-hold files that have been uploaded for Call Park. The customized music-on-hold files for the Call Park application are stored in the file store of the pool. To copy the audio files from a pool file store to a Skype for Business Server 2019 file store, use the **Xcopy** command with the following parameters:

```
Xcopy <Source: legacy Pool CPS File Store Path> <Destination: Skype for Business Server 2019 Pool CPS File Store Path>
```

```
Example usage: Xcopy "<legacy File Store Path>\OcsFileStore\coX-ApplicationServer-X\AppServerFiles\CPS\" " <Skype for Business Server 2019 File Store Path>\OcsFileStore\coX-ApplicationServer-X\AppServerFiles\CPS"
```

When all customized audio files have been copied to the Skype for Business Server 2019 file store, the Call Park application settings of the Skype for Business Server 2019 pool must be configured, and the Call Park orbit ranges that are associated with the legacy pool must be reassigned to the Skype for Business Server 2019 pool.

The Call Park application settings include the pickup timeout threshold, enabling or disabling music on hold, the maximum call pickup attempts, and the timeout request. You must manage Call Park application settings by using the Skype for Business Server Management Shell to run the **Set-CsCpsConfiguration** cmdlet. You cannot manage the Call Park application settings using the Skype for Business Server Control Panel.

## Reconfigure the Call Park Service Settings

1. From the Skype for Business Server 2019 Front End Server, open the Skype for Business Server Management Shell.
2. At the command line, type the following:

### NOTE

If your Skype for Business Server 2019 Call Park application settings are identical to the legacy settings, you can skip this step. If Call Park application settings are different for the Skype for Business Server 2019 and legacy environments, use the cmdlet below as a template to update those changes.

```
Set-CsCpsConfiguration -Identity "<LS2013 Call Park Service ID>" -CallPickupTimeoutThreshold "<LS2010 CPS TimeSpan>" -EnableMusicOnHold "<LS2010 CPS value>" -MaxCallPickupAttempts "<LS2010 CPS pickup attempts>" -OnTimeoutURI "<LS2010 CPS timeout URI>"
```

To reassign all Call Park orbit ranges from the legacy pool to the Skype for Business Server 2019 pool, you can use either the Skype for Business Server Control Panel or the Skype for Business Server Management Shell.



# Reassign all Call Park Orbit Ranges using Skype for Business Server Control Panel

1. Open Skype for Business Server Control Panel.
2. In the left pane, select **Voice Features**.
3. Select the **Call Park** tab.
4. For each Call Park orbit range assigned to a legacy pool, edit the **FQDN of destination server** setting and select the Skype for Business Server 2019 pool that will process the Call Park requests.
5. Select **Commit** to save the changes.

# Reassign all Call Park Orbit Ranges using Skype for Business Server Management Shell

1. Open Skype for Business Server Management Shell.
2. At the command line, type the following:

```
Get-CsCallParkOrbit
```

This cmdlet lists all of the Call Park orbit ranges in the deployment. All Call Park orbits that have the **CallParkServiceId** and **CallParkServerFqdn** parameters set as the legacy pool must be reassigned.

To reassign the legacy Call Park orbit ranges to the Skype for Business Server 2019 pool, at the command line, type the following:

```
Set-CsCallParkOrbit -Identity "<Call Park Orbit Identity>" -CallParkService "service:ApplicationServer:  
<Skype for Business Server 2019 Pool FQDN>"
```

After reassigning all Call Park orbit ranges to the Skype for Business Server 2019 pool, the migration process for the Call Park application will be completed and the Skype for Business Server 2019 pool will handle all future Call Park requests.

# Migrate response groups

8/7/2019 • 5 minutes to read

After your users are moved to Skype for Business Server 2019 pools, you can migrate your response groups. Migrating response groups includes copying agent groups, queues, workflows, audio files, and moving Response Group contact objects from the legacy deployment to the Skype for Business Server 2019 pool. After you migrate your legacy response groups, calls to the response groups are handled by the Response Group application in the Skype for Business Server 2019 pool. Calls to response groups are no longer handled by the legacy pool.

## NOTE

Although you can migrate response groups before you move all users to the Skype for Business Server 2019 pool, we recommend that you move all users first. In particular, users who are response group agents will not have full functionality of new features until they are moved to the Skype for Business Server 2019 pool.

Before you migrate response groups, you must have deployed a Skype for Business Server 2019 pool that includes the Response Group application. The Response Group application is installed and activated by default when you deploy Enterprise Voice. You can ensure that the Response Group application is installed by running the **Get-CsService -ApplicationServer** cmdlet.

## NOTE

You can create new Skype for Business Server 2019 response groups in the Skype for Business Server 2019 pool before you migrate your legacy response groups.

To migrate response groups from a legacy pool to the Skype for Business Server 2019, you run the **Move-CsRgsConfiguration** cmdlet.

## IMPORTANT

The Response Group migration cmdlet moves the Response Group configuration for the entire pool. You cannot select specific groups, queues, or workflows to migrate.

After you migrate the response groups, you need to use Skype for Business Server Control Panel or Skype for Business Server Management Shell cmdlets to verify that all agent groups, queues, and workflows moved successfully.

When you migrate response groups, the legacy response groups are not removed. When you manage response groups after migration by using either Skype for Business Server Control Panel or Skype for Business Server Management Shell, you can see both the legacy response groups and the Skype for Business Server 2019 response groups. You should apply updates only to the Skype for Business Server 2019 response groups. The legacy response groups are retained only for rollback purposes.

## Caution

After the migration has been completed and the new response groups have been created, the Skype for Business Server Control Panel and the Skype for Business Server Management Shell will display the legacy and Skype for Business Server 2019 versions of each response group. Do not use Skype for Business Server Control Panel or Skype for Business Server Management Shell to remove the legacy response groups. If you do remove one, the corresponding response group that was created during migration will stop working. The legacy response groups

will be removed when you decommission the legacy pool.

#### IMPORTANT

We recommend that you do not remove any data from your previous deployment until you decommission the pool. In addition, we strongly recommend that you export response groups immediately after you migrate. If a legacy response group should get removed, you can then restore your response groups from the backup to get Skype for Business Server 2019 response groups running again.

Skype for Business Server 2019 introduces a new Response Group feature called **Workflow Type**. **Workflow Type** can be **Managed** or **Unmanaged**. All response groups are migrated with **Workflow Type** set to **Unmanaged** and with an empty Manager list.

When you run the **Move-CsRgsConfiguration** cmdlet, the agent groups, queues, workflows, and audio files remain in the legacy pool for rollback purposes. If you do need to roll back to the legacy pool, however, you need to run the **Move-CsApplicationEndpoint** cmdlet to move contact objects back to the legacy pool.

The following procedure for migrating Response Group configurations assumes that you have a one-to-one relationship between your legacy pools and the Skype for Business Server 2019 pools. If you plan to consolidate or split up pools during your migration and deployment, you need to plan which legacy pool maps to which Skype for Business Server 2019 pool.

## To migrate Response Group configurations

1. Log on to the computer with an account that is a member of the RTCUniversalServerAdmins group or has equivalent administrator rights and permissions.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Management Shell**.
3. Run:

```
Move-CsRgsConfiguration -Source <source pool FQDN> -Destination <destination pool FQDN>
```

For example:

```
Move-CsRgsConfiguration -Source skype-old.contoso.net -Destination skype-new.contoso.net
```

4. After you migrate response groups and agents to the Skype for Business Server 2019 pool, the URL that agents use to sign in and sign out is a Skype for Business Server 2019 URL and is available from the **Tools** menu. Remind agents to update any references, such as bookmarks, to the new URL.

## To verify Response Group migration by using Skype for Business Server Control Panel

1. Log on to the computer with an account that is a member of RTCUniversalReadOnlyAdmins group or is minimally a member of the CsViewOnlyAdministrator role.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel. For details about the different methods you can use to start Skype for Business Server Control Panel, see [Open Skype for Business Server 2019 administrative tools](#).
3. In the left navigation pane, click **Response Groups**.

4. On the **Workflow** tab, verify that all the workflows in your legacy environment are included in the list.
5. Click the **Queue** tab, and verify that all the queues in your legacy environment are included in the list.
6. Click the **Group** tab, and verify that all the agent groups in your legacy environment are included in the list.

## To verify Response Group migration by using Skype for Business Server Management Shell

1. Log on to the computer with an account that is a member of RTCUniversalReadOnlyAdmins group or is minimally a member of the CsViewOnlyAdministrator role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Management Shell**.

For details about the following cmdlets, run:

```
Get-Help <cmdlet name> -Detailed
```

3. Run:

```
Get-CsRgsAgentGroup
```

4. Verify that all the agent groups in your legacy environment are included in the list.

5. Run:

```
Get-CsRgsQueue
```

6. Verify that all the queues in your legacy environment are included in the list.

7. Run:

```
Get-CsRgsWorkflow
```

8. Verify that all the workflows in your legacy environment are included in the list.

# Migrate Address Book

8/7/2019 • 3 minutes to read

In general, the Address Book is migrated along with the rest of your topology. However, you might need to perform some post-migration steps if you customized the following in your legacy environment:

- Customized the Address Book normalization rules.
- Changed the default value for the **UseNormalizationRules** parameter to False.

## Address Book Normalization Rules

If you customized Address Book normalization rules in your legacy environment, you must migrate the customized rules to your pilot pool. If you did not customize Address Book normalization rules, you have nothing to migrate for Address Book service. The default normalization rules for Skype for Business Server 2019 are the same as the default rules for the legacy install. Follow the procedure later in this section to migrate customized normalization rules.

### NOTE

If your organization uses remote call control and you customized Address Book normalization rules, you must perform the procedure in this topic before you can use remote call control. The procedure requires membership in the RTCUniversalServerAdmins group or equivalent rights.

## UseNormalizationRules Set to False

If you set the value for **UseNormalizationRules** to False so that users can use phone numbers as they are defined in Active Directory Domain Services without having Skype for Business Server 2019 apply normalization rules, you need to set the **UseNormalizationRules** and **IgnoreGenericRules** parameters to True. Follow the procedure later in this section to set these parameters to True.

## To migrate Address Book customized normalization rules

1. Find the `Company_Phone_Number_Normalization_Rules.txt` file in the root of the Address Book shared folder, and copy it to the root of the Address Book shared folder in your Skype for Business Server 2019 pilot pool.

### NOTE

The sample Address Book normalization rules have been installed in your ABS Web component file directory. The path is **`$installedDriveLetter:\Program Files\Microsoft Skype for Business Server 2019\Web Components\Address Book Files\Files\Sample_Company_Phone_Number_Normalization_Rules.txt`**. This file can be copied and renamed as **`Company_Phone_Number_Normalization_Rules.txt`** to the address book shared folder's root directory. For example, the address book shared in **`$serverX`**, the path will be similar to: **`\$serverX\SkypeForBusiness-FileShare\2-WebServices-1\ABFiles`**.

2. Use a text editor, such as Notepad, to open the `Company_Phone_Number_Normalization_Rules.txt` file.
3. Certain types of entries will not work correctly in Skype for Business Server 2019. Look through the file for the types of entries described in this step, edit them as necessary, and save the changes to the Address Book shared folder in your pilot pool.

Strings that include required whitespace or punctuation cause normalization rules to fail because these characters are stripped out of the string that is input to the normalization rules. If you have strings that include required whitespace or punctuation, you need to modify the strings. For example, the following string would cause the normalization rule to fail:

```
\s*(\s*\d\d\s*)\s*\-\s*\d\d\s*\-\s*\d\d
```

The following string would not cause the normalization rule to fail:

```
\s*(?\s*\d\d\s*)?\s*\-\s*\d\d\s*\-\s*\d\d
```

## To set UseNormalizationRules and IgnoreGenericRules to true

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Management Shell**.
2. Do one of the following:
  - If your deployment includes only Skype for Business Server 2019, run the following cmdlet at the global level to change the values for **UseNormalizationRules** and **IgnoreGenericRules** to True:

```
Set-CsAddressBookConfiguration -identity <XdsIdentity> -UseNormalizationRules=$true -  
IgnoreGenericRules=$true
```

- If your deployment includes a combination of Skype for Business Server 2019 and a legacy install, run the following cmdlet and assign it to each Skype for Business Server 2019 pool in the topology:

```
New-CsAddressBookConfiguration -identity <XdsIdentity> -UseNormalizationRules=$true -  
IgnoreGenericRules=$true
```

3. Wait for Central Management store replication to occur on all pools.
4. Modify the phone normalization rules file, "Company\_Phone\_Number\_Normalization\_Rules.txt", for your deployment to clear the content. The file is on the file share of each Skype for Business Server 2019 pool. If the file is not present, then create an empty file named "Company\_Phone\_Number\_Normalization\_Rules.txt".
5. Wait several minutes for all Front End pools to read the new files.
6. Run the following cmdlet on each Skype for Business Server 2019 pool in your deployment:

```
Update-CsAddressBook
```

# Configure the meeting join page

8/7/2019 • 2 minutes to read

When a user clicks a meeting link in a meeting request, the meeting join page detects which client is already installed on the user's computer. If a client is already installed, that client opens and joins the meeting. If a client is not installed, by default the Web App opens.

You can modify the behavior of the meeting join page if you want to allow users to join meetings. These configuration options have been removed from the Control Panel, but you configure them by using the `CsWebServiceConfiguration` cmdlet.

## Meeting Join Page `CsWebServiceConfiguration` Parameters

CSWEBSERVICECONFIGURATION PARAMETER	DESCRIPTION
ShowJoinUsingLegacyClientLink	If set to True, users joining a meeting by using a client application other than Lync will be given the opportunity to join the meeting. The default value is False.
ShowAlternateJoinOptionsExpanded	When set to True, alternate options for joining an online conference will automatically be expanded and shown to users. When set to False (the default value), these options will be available, but the user will have to display the list of options for themselves.

### To configure the meeting join page by using Skype for Business Server 2019 Management Shell

1. Start the Skype for Business Server 2019 Management Shell: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Management Shell**.
2. Run the following cmdlet:

```
Get-CsWebServiceConfiguration
```

This cmdlet returns the web service configuration settings.

3. Run the following command, with the parameters set to True or False, depending on your preference (for details about the parameters for this cmdlet, see the [Skype for Business Server Management Shell](#) documentation):

```
Set-CsWebServiceConfiguration -Identity global -ShowJoinUsingLegacyClientLink $True
```

# Remove legacy Archiving and Monitoring servers

8/7/2019 • 2 minutes to read

If your legacy deployment contained an Archiving Server or a Monitoring Server, after migrating to Skype for Business Server 2019, those servers can be removed from the legacy environment, provided all users have been removed from any remaining legacy pools. You can remove the Archiving Server or Monitoring Server in any sequence. The key requirement is that all users have been removed from any remaining legacy pools.

You can move users to Skype for Business Server 2019 by following the procedures outlined in [Phase 4: Move test users to the pilot pool](#).

After you have confirmed that all users have been removed from any remaining pools, decommission the server and remove roles. A dated, but relevant, example is "Uninstalling Microsoft Lync Server and Removing Server Roles," which can be downloaded at <https://go.microsoft.com/fwlink/p/?linkId=246227>.



# Configure trusted application servers

8/7/2019 • 2 minutes to read

In a mixed environment, if you create a new trusted application server, you must set the next hop pool to be a Skype for Business Server 2019 pool. In a mixed environment, both the legacy pool and the Skype for Business Server 2019 pool appear in the drop-down list. Selecting the legacy pool is not supported.

## IMPORTANT

If you are migrating a trusted application server, you should also update the version of UCMA you are using. If you create a new Trusted Application Pool for Skype for Business Server 2019, you should update UCMA to the version that is included with Skype for Business Server 2019 or the latest version available.

## Select Skype for Business Server 2019 as next hop when creating a Trusted application server

1. Open Topology Builder.
2. In the left pane, right-click **Trusted application servers** and click **New Trusted Application Pool**.
3. Enter the **Pool FQDN** of the trusted application pool and select whether it will be single-server or multiple-server.
4. Click **Next**.
5. On the **Select the next hop** page, from the list, select the Skype for Business Server 2019 Front End pool.
6. Click **Finish**.
7. Select the top node **Skype for Business Server**, and from the **Action** menu select **Publish**.

Verify that the **Trusted Application Pool** has been created successfully and is associated with the correct Front End pool.

# Deploy Skype for Business Server clients

8/7/2019 • 2 minutes to read

For details, see [Deploy clients for Skype for Business Server](#) in the Deployment documentation.

# Connect a Survivable Branch Appliance

8/7/2019 • 2 minutes to read

Every Survivable Branch Appliance (SBA) is associated with a Front End pool that serves as a backup registrar for the SBA. When the Front End pool is migrated to Skype for Business Server 2019, the SBA must be disassociated from the Front End pool while the pool is upgraded. After the pool has been migrated to Skype for Business Server 2019, the SBA can be re-associated with the upgraded Front End pool. This involves deleting the SBA from the legacy topology in Topology Builder and then adding the SBA to the Skype for Business Server 2019 topology. Users homed on the legacy SBA must first be moved to another Front End pool before removing the SBA from the topology. After the SBA is added to the Skype for Business Server 2019 topology, those users can be moved back to the SBA. These steps are summarized below:

1. Move branch users homed on the legacy SBA to another Front End pool.
2. Remove SBA from the legacy topology to disconnect the existing Front End pool as a backup registrar.
3. Add SBA to the Skype for Business Server 2019 topology and configure this new Front End pool as the backup registrar.
4. Move the branch users to the new Skype for Business Server 2019 SBA.

## Add legacy SBA branch site to your topology

1. Open **Topology Builder**.
2. In the left pane, right-click **Branch sites**, and then click **New Branch Site**.
3. In the **Define New Branch Site** dialog box, click **Name**, and then type the name of the branch site.
4. (Optional) Click **Description**, and then type a meaningful description for the branch site.
5. Click **Next**.
6. (Optional) In the next **Define New Branch Site** dialog box, do any of the following:
  - a. Click **City**, and then type the name of the city in which the branch site is located.
  - b. Click **State/Region**, and then type the name of the state or region in which the branch site is located.
  - c. Click **Country Code**, and then type the two-digit calling code for the country/region in which the branch site is located.
7. Click **Next**, and then, if you are using a Survivable Branch Appliance or Server at this site, be sure to clear the **Open the New Survivable Wizard when this wizard closes** check box. Click **Finish**.
8. To associate the legacy SBA to the Skype for Business Server 2019 Front End pool:
  - a. Expand the branch site that has been created.
  - b. Right-click on legacy version, and then click **New**.
  - c. Click **Survivable Branch Appliance**.
9. Follow the directions in the wizard that opens. For information about wizard items, see

**NOTE**

A Survivable Branch Appliance can only be associated with a Monitoring Store.

10. If you are not using a Survivable Branch Appliance or Server at this site, clear the **Open the New Survivable Wizard when this wizard closes** check box, and then click **Finish**.
11. Repeat the previous steps for each branch site you want to add to the topology.

# Configure SCOM monitoring

8/7/2019 • 2 minutes to read

After migrating to Skype for Business Server 2019, you must complete a few tasks to configure Skype for Business Server 2019 to work with System Center Operations Manager.

- Apply updates to a server elected to manage the central discovery logic.
- Update the central discovery candidate server registry key.
- Configure your primary System Center Operations Manager management server to override the candidate central discovery node.

Instructions for carrying out each of these tasks are provided below.

## Apply updates to a server elected to manage the central discovery logic.

1. Elect a server that has the System Center Operations Manager agent files installed and is configured as a candidate discovery node.
2. Apply updates to this server. See the topic [Apply updates](#).

## Update the central discovery candidate server registry key.

1. On the server elected to manage the central discovery logic, open a Windows PowerShell command window.
2. At the command line, type the following:

```
New-Item -Path "HKLM:\Software\Microsoft\Real-Time Communications\Health"
```

```
New-Item -Path "HKLM:\Software\Microsoft\Real-Time Communications\Health\CentralDiscoveryCandidate"
```

### NOTE

Whenever you edit the registry, you may experience an error that the command failed if the registry key already exists. If you experience this, you can safely ignore the error.

## Configure your primary System Center Operations Manager management server to override the candidate central discovery watcher node.

1. On a computer where the System Center Operations Manager console has been installed, expand **Management Pack Objects** and then select **Object Discoveries**.
2. Click **Change Scope**
3. From the **Scope Management Pack Objects** page, select **LS Discovery Candidate**.
4. Override the **LS Discovery Candidate Effective Value** to the name of the candidate server elected in the earlier procedure.

To finalize your changes, restart the health service on the System Center Operations Manager Root Management Server.

# Migrate Common Area Phones

8/7/2019 • 2 minutes to read

Common Area Phones are IP phones that most often reside in a shared workspace or common area, like a lobby, kitchen, or factory floor. Common Area Phones do not need to be connected to a computer to provide Skype for Business Server unified communications (UC) functionality. After migrating a deployment to Skype for Business Server 2019, you must also migrate the contact objects associated with the legacy Common Area Phone. Using Skype for Business Server Management Shell, you will first retrieve all contact objects associated with the legacy Common Area Phones, and then move those objects to the Skype for Business Server 2019 pool.

## Migrate Common Area Phones

1. From the Skype for Business Server 2019 Front End server, open Skype for Business Server Management Shell.
2. From the command line, type the following:

```
Get-CsCommonAreaPhone -Filter {RegistrarPool -eq "pool01.contoso.net"} | Move-CsCommonAreaPhone -Target pool02.contoso.net
```

3. To verify that all contact objects have been moved to the Skype for Business Server 2019 pool, from the Skype for Business Server Management Shell type the following:

```
Get-CsCommonAreaPhone -Filter {RegistrarPool -eq "pool02.contoso.net"}
```

Verify that all contact objects are now associated with the Skype for Business Server 2019 pool.

# Migrate analog devices

8/7/2019 • 2 minutes to read

Skype for Business Server provides support for analog devices. Specifically, the supported analog devices are analog audio phones and analog fax machines. You can configure the qualified gateways to support the use of analog devices in your Skype for Business Server environment. After you migrate to Skype for Business Server 2019, you must also migrate the contact objects associated with the analog devices. Use Skype for Business Server Management Shell to first retrieve all contact objects associated with the legacy analog devices, and then move those objects to the Skype for Business Server 2019 pool.

## To migrate analog devices

1. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Skype for Business Server 2019**, and then click **Skype for Business Server Management Shell**.
2. At the command line, type:

```
Get-CsAnalogDevice -Filter {RegistrarPool -eq "pool01.contoso.net"} | Move-CsAnalogDevice -Target pool02.contoso.net
```

3. Verify that all contact objects have been moved to the Skype for Business Server 2019 pool. At the command line, type:

```
Get-CsAnalogDevice -Filter {RegistrarPool -eq "pool02.contoso.net"}
```

4. Verify that all the contact objects are now associated with the Skype for Business Server 2019 pool.

# Phase 8: Decommission legacy pools

8/7/2019 • 2 minutes to read

The following topic provides guidance for updating DNS entries, moving the Content Management Server, decommissioning pools, and deactivating and removing servers and pools from a legacy deployment. Not all of the procedures listed in this section are required. Read the documentation and determine which decommissioning procedure to use.

For a dated but exhaustive article on removing servers and server roles, and a step-by-step guide to decommissioning a deployment, download [Uninstalling Microsoft Lync Server and Removing Server Roles](#).

## IMPORTANT

For information on migrating and upgrading Microsoft Unified Communications Managed API (UCMA) applications, before decommissioning your legacy environment, see [UCMA applications: Coexistence, migration, and upgrade scenarios](#).

## In this section

[Update DNS SRV records](#)

[Move the legacy install Central Management Server to Skype for Business Server 2019](#)

[Move Conference Directories](#)

[Remove the Archiving server association](#)

[Remove the Monitoring server association](#)

[Remove the Enterprise Edition Front End Server or Standard Edition Front End Server](#)

[Remove SQL Server instances and databases on the Back End Server](#)



# Update DNS SRV records

8/7/2019 • 2 minutes to read

To successfully complete this procedure, you should be logged on to the server or domain as a member of the Domain Admins group or a member of the DnsAdmins group.

This topic describes how to update the Domain Name System (DNS) records after migrating to Skype for Business Server 2019. After all users have been moved to Skype for Business Server 2019, but before the legacy pool or Director is decommissioned, you must update the DNS SRV records in your internal DNS for every SIP domain. This procedure assumes that your internal DNS has zones for your SIP user domains.

## To configure a DNS SRV record

1. On the DNS server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your SIP domain, expand **Forward Lookup Zones**, expand the SIP domain in which Skype for Business Server 2019 is installed, and navigate to the **\_tcp** setting.
3. In the right pane, right-click **\_sipinternaltls** and select **Properties**.
4. In **Host offering this service**, update the host FQDN to point to the Skype for Business Server 2019 pool.
5. Click **OK**.

## To verify that the FQDN of the Front End pool or Standard Edition server can be resolved

1. Log on to a client computer in the domain.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type `cmd`, and then click **OK**.
4. At the command prompt, type `nslookup <FQDN of the Front End pool> or <FQDN of the Standard Edition server>`, and then press ENTER.
5. Verify that you receive a reply that resolves to the appropriate IP address for the FQDN.

# Move the legacy Central Management Server to Skype for Business Server 2019

10/9/2019 • 6 minutes to read

After migrating to Skype for Business Server 2019, and before you can remove the legacy server, you need to move the Central Management Server to the Skype for Business Server 2019 Front End Server or pool.

The Central Management Server is a single master/multiple replica system, where the read/write copy of the database is held by the Front End Server that contains the Central Management Server. Each computer in the topology, including the Front End Server that contains the Central Management Server, has a read-only copy of the Central Management store data in the SQL Server database (named RTCLOCAL by default) installed on the computer during setup and deployment. The local database receives replica updates by way of the Skype for Business Server Replica Replicator Agent that runs as a service on all computers. The name of the actual database on the Central Management Server and the local replica is XDS, which is made up of the xds.mdf and xds.ldf files. The master database location is referenced by a service control point (SCP) in Active Directory Domain Services. All tools that use the Central Management Server to manage and configure Skype for Business Server use the SCP to locate the Central Management store.

After you have successfully moved the Central Management Server, you should remove the Central Management Server databases from the original Front End Server. For information on removing the Central Management Server databases, see [Remove the SQL Server database for a Front End pool](#).

You use the Windows PowerShell cmdlet **Move-CsManagementServer** in the Skype for Business Server Management Shell to move the database from the legacy install SQL Server database to the Skype for Business Server 2019 SQL Server database, and then update the SCP to point to the Skype for Business Server 2019 Central Management Server location.

Use the procedures in this section to prepare the Skype for Business Server 2019 Front End Servers before you move the Central Management Server.

## To prepare an Enterprise Edition Front End pool

1. On the Skype for Business Server 2019 Enterprise Edition Front End pool where you want to relocate the Central Management Server, log on to the computer where the Skype for Business Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group. You must also have SQL Server database sysadmin user rights and permissions on the database where you want to install the Central Management store.
2. Open the Skype for Business Server Management Shell.
3. To create the new Central Management store in the Skype for Business Server 2019 SQL Server database, in the Skype for Business Server Management Shell, type:

```
Install-CsDatabase -CentralManagementDatabase -SQLServerFQDN <FQDN of your SQL Server> -SQLInstanceName <name of instance>
```

4. Confirm that the status of the **Skype for Business Server Front-End** service is **Started**.

## To prepare a Standard Edition Front End Server

1. On the Skype for Business Server 2019 Standard Edition Front End Server where you want to relocate the Central Management Server, log on to the computer where the Skype for Business Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group.
2. Open the Skype for Business Server Deployment Wizard.
3. In the Skype for Business Server Deployment Wizard, click **Prepare first Standard Edition server**.
4. On the **Executing Commands** page, SQL Server Express is installed as the Central Management Server. Necessary firewall rules are created. When the installation of the database and prerequisite software is completed, click **Finish**.

#### NOTE

The initial installation may take some time with no visible updates to the command output summary screen. This is due to the installation of SQL Server Express. If you need to monitor the installation of the database, use Task Manager to monitor the setup.

5. To create the new Central Management store on the Skype for Business Server 2019 Standard Edition Front End Server, in the Skype for Business Server Management Shell, type:

```
Install-CsDatabase -CentralManagementDatabase -SQLServerFQDN <FQDN of your Standard Edition Server> -  
SQLInstanceName <name of instance - RTC by default>
```

6. Confirm that the status of the **Skype for Business Server Front-End** service is **Started**.

## To move the legacy installs Central Management Server to Skype for Business Server 2019

1. On the Skype for Business Server 2019 server that will be the Central Management Server, log on to the computer where the Skype for Business Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group. You must also have the SQL Server database administrator user rights and permissions.
2. Open Skype for Business Server Management Shell (run as administrator).
3. In the Skype for Business Server Management Shell, type:

```
Enable-CsTopology
```

#### Caution

If `Enable-CsTopology` is not successful, resolve the problem preventing the command from completing before continuing. If **Enable-CsTopology** is not successful, the move will fail and it may leave your topology in a state where there is no Central Management store.

4. On the Skype for Business Server 2019 Front End Server or Front End pool, in the Skype for Business Server Management Shell, type:

```
Move-CsManagementServer
```

5. Skype for Business Server Management Shell displays the servers, file stores, database stores, and the service connection points of the Current State and the Proposed State. Read the information carefully and confirm that this is the intended source and destination. Type **Y** to continue, or **N** to stop the move.

- Review any warnings or errors generated by the **Move-CsManagementServer** command and resolve them.
- On the Skype for Business Server 2019 server, open the Skype for Business Server Deployment Wizard.
- In Skype for Business Server Deployment Wizard, click **Install or Update Skype for Business Server System**, click **Step 2: Setup or Remove Skype for Business Server Components**, click **Next**, review the summary, and then click **Finish**.
- On the legacy install server, open the Deployment Wizard.
- In Skype for Business Server Deployment Wizard, click **Install or Update Skype for Business Server System**, click **Step 2: Setup or Remove Skype for Business Server Components**, click **Next**, review the summary, and then click **Finish**.
- Reboot the Skype for Business Server 2019 server. This is required because of a group membership change to access Central Management Server database.
- To confirm that replication with the new Central Management store is occurring, in the Skype for Business Server Management Shell, type:

```
Get-CsManagementStoreReplicationStatus
```

#### NOTE

The replication may take some time to update all current replicas.

## To remove legacy install Central Management store files after a move

- On the legacy install server, log on to the computer where the Skype for Business Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group. You must also have the SQL Server database administrator user rights and permissions.
- Open Skype for Business Server Management Shell

**Caution**  
Do not proceed with the removal of the previous database files until replication is complete and is stable. If you remove the files prior to completing replication, you will disrupt the replication process and leave the newly moved Central Management Server in an unknown state. Use the cmdlet **Get-CsManagementStoreReplicationStatus** to confirm the replication status.
- To remove the Central Management store database files from the legacy install Central Management Server, type:

```
Uninstall-CsDatabase -CentralManagementDatabase -SqlServerFqdn <FQDN of SQL Server> -SqlInstanceName <Name of source server>
```

For example:

```
Uninstall-CsDatabase -CentralManagementDatabase -SqlServerFqdn sql.contoso.net -SqlInstanceName rtc
```

Where the *<FQDN of SQL Server>* is either the legacy install Back End Server in an Enterprise Edition deployment or the FQDN of the Standard Edition server.

# Move Conference Directories

8/7/2019 • 2 minutes to read

Before decommissioning a pool, you must perform the following procedure for each conference directory in your legacy pool.

## To Move a Conference Directory to Skype for Business Server 2019

1. Open the Skype for Business Server Management Shell.
2. To obtain the identity of the conference directories in your organization, run the following command:

```
Get-CsConferenceDirectory
```

The preceding command returns all the conference directories in your organization. Because of that, you might want to limit the results to the pool being decommissioned. For example, if you are decommissioning the pool with the fully qualified domain name (FQDN) pool01.contoso.net, use this command to limit the returned data to conference directories from that pool:

```
Get-CsConferenceDirectory | Where-Object {$_.ServiceID -match "pool01.contoso.net"}
```

That command returns only the conference directories where the ServiceID property contains the FQDN pool01.contoso.net.

3. To move conference directories, run the following command for each conference directory in the pool:

```
Move-CsConferenceDirectory -Identity <Numeric identity of conference directory> -TargetPool <FQDN of pool where ownership is to be transitioned>
```

For example, to move conference directory 3, use this command, specifying a Skype for Business Server 2019 pool as the TargetPool:

```
Move-CsConferenceDirectory -Identity 3 -TargetPool "pool02.contoso.net"
```

If you want to move all the conference directories on a pool, use a command similar to the following:

```
Get-CsConferenceDirectory | Where-Object {$_.ServiceID -match "pool01.contoso.net"} | Move-CsConferenceDirectory -TargetPool "pool02.contoso.net"
```

Download [Uninstalling Microsoft legacy and Removing Server Roles](#) for comprehensive, step-by-step instructions on decommissioning legacy pools.

When moving conference directories, you might encounter the following error:

```
WARNING: Move operation failed for conference directory with ID "5". Cannot perform a rollback because data migration might have already started. Retry the operation.
WARNING: Before using the -Force parameter, ensure that you have exported the conference directory data using DBImpExp.exe and imported the data on the target pool. Refer to the DBImpExp-Readme.htm file for more information.
Move-CsConferenceDirectory : Unable to cast COM object of type 'System._ComObject' to interface type 'Microsoft.Rtc.Interop.User.IRtcConfDirManagement'.
This operation failed because the QueryInterface call on the COM component for the interface with SID '{4262B886-503F-4BEA-868C-04E8DF562CEB}' failed due to the following error: The specified module could not be found.
```

This error typically occurs when the Skype for Business Server Management Shell requires an updated set of Active Directory permissions in order to complete a task. To resolve the problem, close the current instance of the Management Shell, then open a new instance of the shell and re-run the command to move the conference directory.

# Remove the Archiving server association

8/7/2019 • 2 minutes to read

To remove an Archiving Server, you need to change or clear the dependency on the associated Front End pool, Front End Server, Survivable Branch Appliance, and Survivable Branch Server. You edit the properties of the Front End pool, Front End Server, Survivable Branch Appliance, and Survivable Branch Server to remove the dependency. After you clear the dependency and delete the server in Topology Builder, you are notified that the associated database store object in Topology Builder will also be deleted.

## To remove the Archiving Server association

1. On the Skype for Business Server 2019 Front End Server, open Topology Builder.
2. Navigate to the legacy install node.
3. In Topology Builder, expand **Enterprise Edition Front End pools, Standard Edition Front End Servers,** or **Branch sites**, depending on where the Archiving Server is defined.
4. If you have Survivable Branch Server associated, expand **Branch sites**, expand the branch site name, and then expand **Survivable Branch Appliances**.

### NOTE

**Survivable Branch Appliances** in the user interface applies to both Survivable Branch Server and Survivable Branch Appliance.

5. Right-click the pool, server, or device that is associated with the Archiving Server, and then click **Edit Properties**.
6. In **Edit Properties**, under **General > Associations**, clear the **Associate Archiving Server** check box, and then click **OK**.
7. Repeat the previous step for any other pool, server, or device associated with the Archiving Server that you want to remove.
8. Right-click the Archiving Server, and then click **Delete**.
9. On **Delete Dependent Stores**, click **OK**.
10. Publish the topology, check replication status, and then run the Skype for Business Server Deployment Wizard as needed.

# Remove the Monitoring server association

8/7/2019 • 2 minutes to read

To remove the Monitoring Server, you need to change or clear the dependency on the associated Front End pool, Front End Server, Survivable Branch Appliance, and Survivable Branch Server. You edit the properties of the Front End pool, Front End Server, Survivable Branch Appliance, and Survivable Branch Server to remove the dependency. After you clear the dependency and delete the server in Topology Builder, you are notified that the associated database store object in Topology Builder will also be deleted.

## To remove the Monitoring Server association

1. On the Skype for Business Server 2019 Front End Server, open Topology Builder.
2. Navigate to the legacy installs node.
3. In Topology Builder, expand **Enterprise Edition Front End pools, Standard Edition Front End Servers,** or **Branch sites**, depending on where the Monitoring Server is defined.
4. If you have Survivable Branch Server associated, expand **Branch sites**, expand the branch site name, and then expand **Survivable Branch Appliances**.

### NOTE

**Survivable Branch Appliances** in the user interface applies to both Survivable Branch Server and Survivable Branch Appliance.

5. Right-click the pool, server, or device that is associated with the Monitoring Server, and then click **Edit Properties**.
6. In **Edit Properties**, under **General > Associations**, clear the **Associate Monitoring Server** check box, and then click **OK**.
7. Repeat the previous step for any other pool, server, or device associated with the Monitoring Server.
8. Right-click the Monitoring Server, and then click **Delete**.
9. On **Delete Dependent Stores**, click **OK**.
10. Publish the topology, check replication status, and run the Skype for Business Server Deployment Wizard as needed.



# Remove the Front End Server

8/7/2019 • 2 minutes to read

The procedures outlined in this section are designed to guide you through the process of removing an Enterprise Edition Front End pool or a Standard Edition Front End Server. After migrating to Skype for Business Server 2019, this is one of the first steps in decommissioning your legacy environment.

## In this section

- [Reset call admission control](#)
- [Prevent sessions for services](#)
- [Stop legacy services](#)
- [Remove a Front End Server from a pool](#)
- [Remove Front End pool or Standard Edition server](#)

# Reset call admission control

8/7/2019 • 2 minutes to read

If a legacy Front End pool is hosting call admission control (CAC), you must move CAC hosting to a Skype for Business Server 2019 pool before you can remove the legacy Front End pool.

## To reset CAC

1. Open Topology Builder.
2. Right-click the site node, and then click **Edit Properties**.
3. Under **Call Admission Control setting**, make sure **Enable Call Admission Control** is selected.
4. Under **Front End pool to run call admission control (CAC)**, select the Skype for Business Server 2019 pool that is to host CAC, and then click **OK**.
5. Publish the topology.

# Prevent sessions for services

8/7/2019 • 2 minutes to read

You can use the legacy installs Control Panel to prevent new sessions for all the legacy services running on a specific computer or to prevent new sessions for a specific legacy service.

## To prevent new sessions for services on a computer

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server 2019.
2. Open Skype for Business Control Panel.
3. In the left navigation bar, click **Topology**, and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the services for which you want to prevent new sessions, and then click it.
5. Click **Action**.
6. Click **Prevent new sessions for all services**.

## To prevent new sessions for a specific service

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server 2019.
2. Open Skype for Business Control Panel.
3. In the left navigation bar, click **Topology**, and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
5. Click **Properties**.
6. Sort the list of services, if necessary, and click the service for which you want to prevent new sessions.
7. Click **Action**.
8. Click **Prevent new sessions for service**.
9. Click **Close**.

# Stop legacy services

8/7/2019 • 2 minutes to read

You can use Skype for Business Server Control Panel to start or stop all the legacy services running on a specific computer or to start or stop a specific legacy service.

## To start or stop all Skype for Business Server services on a computer

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Topology**, and then click **Status**.
3. On the **Status** page, sort or search through the list as needed to find the computer that is running the services you want to start or stop, and then click it.
4. Click **Action**.
5. Click **Start All services** or **Stop All services**.

## To start or stop a specific service

1. Open Skype for Business Server Control Panel.
2. In the left navigation bar, click **Topology**, and then click **Status**.
3. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
4. Click **Properties**.
5. Sort the list of services, if necessary, and click the service you want to start or stop.
6. Click **Action**.
7. Click **Start service** or **Stop service**.
8. Click **Close**.

# Remove a Front End Server from a pool

8/7/2019 • 2 minutes to read

The Front End Server cannot exist as a stand-alone computer. It must be defined as a Front End pool, even if there is only a single computer in the pool.

This topic guides you through the process of removing an individual Front End Server from an existing Front End pool. If the Front End Server is the last server in the pool or if you are removing the pool completely, see [Remove Front End pool or Standard Edition server](#). There is no need to remove the individual Front End Servers before you remove the Front End pool. When you remove the pool, you remove each Front End Server.

## To remove a Front End Server from a pool

1. On the Skype for Business Server 2019 Front End Server, open Topology Builder.
2. Navigate to the legacy install node.
3. Expand **Enterprise Edition Front End pools**, expand the Front End pool with the Front End Server that you want to remove, right-click the Front End Server that you want to remove, and then click **Delete**.

# Remove Front End pool or Standard Edition server

8/7/2019 • 2 minutes to read

This article guides you through the process of removing a Front End pool or a Standard Edition Front End Server. When you remove a Front End pool, you remove each Front End Server that belongs to the pool as a part of the pool removal process. When you remove a Standard Edition Front End Server, you must remove the SQL Store definition from Topology Builder.

## To remove a Front End Server pool

1. Open Topology Builder.
2. Navigate to the legacy node.
3. Expand **Enterprise Edition Front End pools**, expand the Front End pool, right-click the Front End pool that you want to remove, and then click **Delete**.
4. Publish the topology, check replication status, and then run the legacy Deployment Wizard as needed.

## To remove a Standard Edition Front End server

1. Open Topology Builder.
2. Navigate to the legacy installs node.
3. Expand **Standard Edition Front End servers**, right-click the Front End Server that you want to remove, and then click **Delete**.
4. Expand **SQL stores**, right-click the SQL Server database that is associated with the Standard Edition Front End Server, and then click **Delete**.

### IMPORTANT

You must remove the definition of the collocated SQL Server databases from the Standard Edition Front End Server.

5. Publish the topology, check replication status, and then run the Deployment Wizard as needed.

# Remove SQL Server instances and databases on the Back End Server

8/7/2019 • 2 minutes to read

You remove the Microsoft SQL Server databases and instances after you remove the servers running that are dependent on them, or after you reconfigure the servers to use another database. You need to perform the procedure in this topic when you retire the current SQL Server or reconfigure the current server in such a way that it renders the databases obsolete or unavailable.

To remove the databases or instances for the Archiving Server or Monitoring Server, you must first remove the server role. Similarly, to remove the instances or databases for Front End pool, you must first remove or reconfigure the dependent server role. These procedures make no distinction between collocated databases or separate instances for servers. The procedures are unaffected by the collocation of databases.

## In this section

- [Remove the SQL Server database for a Front End pool](#)
- [Remove the SQL Server database for a Monitoring server](#)
- [Remove the SQL Server database for an Archiving server](#)

# Remove the SQL Server database for a Front End pool

8/7/2019 • 2 minutes to read

After you remove a Front End pool or reconfigure the pool to use a different database, you can remove the SQL Server databases that hosted the pool data. Use the following procedures to remove the definitions from Topology Builder, and then remove the database and log files from the database server.

## To remove the SQL Server database using Topology Builder

1. From the Skype for Business Server 2019 Front End Server, open Topology Builder and download the existing topology.
2. In Topology Builder, navigate to **Shared Components** and then **SQL Server Stores**, right-click the SQL Server instance associated with the removed or reconfigured Front End pool, and then click **Delete**.
3. Publish the topology, and then check the replication status.

## To remove user and application databases from the SQL server

1. To remove the databases on the SQL server, you must be a member of the SQL Server sysadmins group for the SQL server where you are removing the database files.
2. Open Skype for Business Server Management Shell.
3. To remove the database for the pool user store, type:

```
Uninstall-CsDataBase -DatabaseType User -SqlServerFqdn <FQDN> [-SqlInstanceName <instance>]
```

Where *<FQDN>* is the fully qualified domain name (FQDN) of the database server, and *<instance>* is the named database instance (that is, if one was defined).

4. To remove the database for the pool application store, type:

```
Uninstall-CsDataBase -DatabaseType Application -SqlServerFqdn <FQDN> [-SqlInstanceName <instance>]
```

Where *<FQDN>* is the FQDN of the database server, and *<instance>* is the named database instance (that is, if one was defined).

5. When the **Uninstall-CsDataBase** cmdlet prompts you to confirm actions, read the information, and then press Y (or Enter) to proceed, or press N and then Enter if you want to stop the cmdlet (if there are errors).



# Remove the SQL Server database for a Monitoring server

8/7/2019 • 2 minutes to read

After you remove a Monitoring Server, you can remove the SQL Server databases that hosted the server data. Use the following procedures to remove the definitions from Topology Builder, and then remove the database and log files from the database server.

## To remove the SQL Server database using Topology Builder

1. On the Skype for Business Server 2019 Front End Server, open Topology Builder.
2. In Topology Builder, navigate to **Shared Components** and then **SQL Server Stores**, right-click the SQL Server instance associated with the removed or reconfigured Monitoring Server, and then click **Delete**.
3. Publish the topology, and then check replication status.

## To remove the database files from the SQL Server

1. To remove the databases on the SQL Server-based server, you must be a member of the SQL Server sysadmins group for the SQL Server server where you are removing the database files.
2. Open the Skype for Business Server Management Shell.
3. At the command line, type the following:

```
Uninstall-CsDataBase -DatabaseType Monitoring -SqlServerFqdn <FQDN> [-SqlInstanceName <instance>]
```

Where *<FQDN>* is the fully qualified domain name (FQDN) of the database server, and *<instance>* is the optional named database instance.

4. When the **Uninstall-CsDataBase** cmdlet prompts you to confirm actions, read the information, and then press Y (or Enter) to proceed, or press N and then Enter if you want to stop the cmdlet (if there are errors).

# Remove the SQL Server database for an Archiving server

8/7/2019 • 2 minutes to read

After you remove an Archiving Server, you can remove the SQL Server databases that hosted the pool data. Use the following procedures to remove the definitions from Topology Builder, and then remove the database and log files from the database server.

## To remove the SQL Server database using Topology Builder

1. On the Skype for Business Server 2019 Front End Server, open Topology Builder.
2. In Topology Builder, navigate to **Shared Components** and then **SQL Server Stores**, right-click the SQL Server instance associated with the removed or reconfigured Archiving Server, and then click **Delete**.
3. Publish the topology, and then check replication status.

## To remove the database files from the SQL Server

1. To remove the databases on the SQL Server, you must be a member of the SQL Server sysadmins group for the SQL Server where you are removing the database files.
2. Open the Skype for Business Server Management Shell.
3. At the command line, type the following:

```
Uninstall-CsDataBase -DatabaseType Archiving -SqlServerFqdn <FQDN> [-SqlInstanceName <instance>]
```

Where *<FQDN>* is the fully qualified domain name (FQDN) of the database server, and *<instance>* is the named database instance (that is, if one was defined).

4. When the **Uninstall-CsDataBase** cmdlet prompts you to confirm actions, read the information, and then press Y (or Enter) to proceed, or press N and then Enter if you want to stop the cmdlet (if there are errors).

# Manage your topology in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the steps to manage your topology in Skype for Business Server.

The following topics provide step-by-step instructions on tasks involved with managing your Skype for Business Server topology and your Front End Servers.

- [Manage Front End Servers](#)
- [Manage databases with an AlwaysOn Availability Group](#)
- [Patch or update a Back End Server or Standard Edition server](#)
- [Move File Store Data to a New File Store](#)
- [Manage services](#)

# Manage Front End Servers in Skype for Business Server

5/20/2019 • 2 minutes to read

This article explains how to add or remove Front End Servers and how to apply upgrades or patches to Front End Servers.

## Add or remove Front End Servers

When you add a Front End Server to a pool, or remove a Front End Server from a pool, you then need to restart the pool.

### IMPORTANT

When you add or remove a server to the pool in your topology and then publish the updated topology, it will cause all of the servers in the pool to restart at the same time. While the servers are restarting the pool is offline, which will interrupt service for your users connected to that pool. To prevent any interruption of service to users, plan to publish the topology with the new server in the pool during non-business hours.

You can use the following procedure when adding or removing a Front End Server.

### NOTE

If you're adding new servers to the pool, update your new pool servers to be at the same Cumulative Update level as the existing servers in the Pool.

### To add or remove Front End Servers

1. If you are removing any Front End Servers, first stop new connections to those servers. To do so, you can use the following cmdlet:

```
Stop-CsWindowsService -Graceful
```

2. Open Topology Builder, and add or remove the necessary servers.
3. Publish the topology.

### IMPORTANT

When you add or remove a server to the pool in your topology and then publish the updated topology, it will cause all of the servers in the pool to restart at the same time. While the servers are restarting the pool is offline, which will interrupt service for your users connected to that pool. To prevent any interruption of service to users, plan to publish the topology with the new server in the pool during non-business hours.

### NOTE

Also, when you add or remove a server to the pool, you must run the Skype for Business Server Deployment Wizard on each computer added or removed, for more information, see [Install Skype for Business Server on servers in the topology](#)

4. If you have changed the number of servers in your Front End pool in any of the following ways, then reset the pool with by typing the following cmdlet: Reset-CsPoolRegistrarState -ResetType FullReset -PoolFqdn

```
Reset-CsPoolRegistrarState -ResetType FullReset -PoolFqdn <PoolFQDN>
```

- 2 to any
- Any to 2
- 3 to any
- Any to 3

5. Restart the pool by typing the following cmdlet

```
Start-CsPool
```

## Patch or update Front End Servers

When you patch the servers in a Front End pool, you do so one server at a time.

### To apply an upgrade to the Front End servers in a pool

1. Type the following cmdlet:

```
Get-CsPoolFabricState -PoolFqdn <PoolFQDN>
```

If this cmdlet shows any missing replicas, then run the following cmdlet to recover the pool before you apply any patches.

```
Reset-CsPoolRegistrarState -ResetType QuorumLossRecovery
```

2. On the first server you want to patch, run the following cmdlet:

```
Invoke-CsComputerFailOver -ComputerName <Front End Server to be patched>
```

This cmdlet moves all services to other Front End Servers in the pool, and takes this server offline.

3. Apply the upgrade or patch to this server.
4. On the upgraded server, run the following cmdlet:

```
Invoke-CsComputerFailBack -ComputerName <Front End Server to be patched>
```

The server is returned to service.

5. Repeat Steps 2-4 for each server that needs to be upgraded.

# Patch or update a Back End Server or Standard Edition server in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to install an update or patch on a Back End Server in Skype for Business Server.

This topic explains how to install an update on an Enterprise Edition Back End Server or a Standard Edition server.

If a Back End Server is down for at least 30 minutes while you are upgrading it, users may then go into resiliency mode. When the upgrade is finished and the Back End Servers has again connected with the Front End Servers in the pool, users are returned to full functionality. If the upgrade takes less than 30 minutes, users will not be affected.

## To update a back end server or Standard Edition server

1. Log on to the server you are upgrading as a member of the CsAdministrator role.
2. Download the update and extract it to the local hard disk.
3. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business**, and then click **Skype for Business Server Management Shell**.
4. Stop Skype for Business Server services. At the command line, type:

```
Stop-CsWindowsService
```

5. Stop the World Wide Web service. At the command line, type:

```
net stop w3svc
```

6. Close all Skype for Business Server Management Shell windows.
7. Install the update.
8. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business**, and then click **Skype for Business Server Management Shell**.
9. Stop Skype for Business Server services again to catch Global Assembly Cache (GAC) -d assemblies. At the command line, type:

```
Stop-CsWindowsService
```

10. Restart the World Wide Web service. At the command line, type:

```
net start w3svc
```

11. Apply the changes made to the SQL Server databases by doing one of the following:

- If this is an Enterprise Edition Back End Server and there are no collocated databases on this server, such as Archiving or Monitoring databases, then type the following at a command line:

```
Install-CsDatabase -Update -ConfiguredDatabases -SqlServerFqdn <SQL Server FQDN>
```

- If this is an Enterprise Edition Back End Server and there are collocated databases on this server, then type the following at a command line:

```
Install-CsDatabase -Update -ConfiguredDatabases -SqlServerFqdn <SQL Server FQDN> -  
ExcludeCollocatedStores
```

- If this is an Standard Edition server, type the following at a command line:

```
Install-CsDatabase -Update -LocalDatabases
```

# Manage databases with an AlwaysOn Availability Group in Skype for Business Server

5/20/2019 • 2 minutes to read

Use the steps in this article to add more Skype for Business Server databases to an existing AlwaysOn Availability Group in Skype for Business Server, and find out about the necessary additional steps after you patch or upgrade a Back End Server that is part of a AlwaysOn Availability Group in Skype for Business Server.

## Add databases to an AlwaysOn Availability Group

1. Open SQL Server Management Studio, and navigate to the AlwaysOn Availability Group. Fail it over to the primary replica.
2. In Topology Builder, set the SQL Server FQDN of the AlwaysOn Availability Group to the FQDN of the primary node of that group.
  - Open Topology Builder, select **Download topology from existing deployment**, and click **OK**.
  - Expand Skype for Business Server, expand your topology, and expand **SQL Server Stores**. Right-click the SQL store of the new AlwaysOn Availability Group, and click **Edit Properties**.
  - At the bottom of the page, in the **SQL Server FQDN** box, type in the FQDN of the primary node of the AlwaysOn Availability Group.
3. Publish the topology. From the **Action** menu click **Topology** and then **Publish**. Then in the confirmation page click **Next**.
4. Use SQL Server Management Studio to add the new database to the AlwaysOn Availability Group.

## Patch or update a SQL Server in an AlwaysOn Availability Group

After patching a Back End Server that is part of an AlwaysOn Availability Group, you must republish the topology.

1. Install the update on your Skype for Business server or servers.
2. Run the following PowerShell command in your Skype for Business Management Shell (logged in with an account that's appropriately permissioned to apply changes to the SQL AlwaysOn databases) as follows:

```
Install-CsDatabase -Update -ConfiguredDatabases -SqlServerFqdn [sqlpool.contoso.com] -Verbose
```

Where [sqlpool.contoso.com] is replaced with the fully qualified domain name (FQDN) of your AlwaysOn availability group.



# Move File Store Data to a New File Store in Skype for Business Server

5/20/2019 • 3 minutes to read

If you need to remove the file server that is currently acting as the file store for your Skype for Business Server deployment, or if you need to make other changes that would make the current file store unavailable, you first need to create a new share. Then you need to perform the following steps:

1. Shut down the Skype for Business Server services that use the file store that you plan to remove.
2. Define the file store in Topology Builder and publish the changes to make the new file store available to your deployment.
3. Move the data to the new file store.
4. Restart the servers or services.
5. Optionally, remove the old file share and file folder.

## To move file store data from one file store to a new file store

1. Log on to a computer as a member of the RTCUniversalServerAdmins or CsServerAdministrator group where the Skype for Business Server, Administrative Tools are installed.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology**, and then click **Status**.
4. For each Director pool, Director, Standard Edition server, and Front End pool that uses the file store that you plan to remove, select the server or pool, click **Action**, and then click **Stop all services**.
5. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
6. Start Topology Builder: Click **Start**, click **All Programs**, click **Skype for Business Server**, and then click **Skype for Business Server Topology Builder**.
7. Select a server or pool that uses the file store, and do the following:
  - a. Right-click the server or pool, and then click **Edit Properties**.
  - b. In **Edit properties**, under **Associations**, under **File store**, click **New**.
  - c. In **Define New File Store**, under **File server FQDN**, type the fully qualified domain name (FQDN) of the file server. Under **File share**, type the folder name for the new file share, and then click **OK**.

### IMPORTANT

This step defines a new file store for use in Topology Builder. You define it only once, not for each server. Before you publish the topology, you must create the defined file share on the defined file server. For details, see [Define the File Store for the Front End](#).

8. For each server or pool that uses the file store, do the following:

- a. Right-click the server or pool, and then click **Edit properties**.
- b. In **Edit Properties**, under **Associations**, in **File store**, select the new file share, and then click **OK**.
9. Publish the topology, check replication status, and then run the Skype for Business Server Deployment Wizard as needed. For details, see [Common Procedures for Removing Lync Servers and Components](#).
10. Start a command prompt: Click **Start**, click **Run**, and then type cmd.exe.
11. At the command line, type the following:

```
Robocopy \\<OldFileServer>\<OldShare> \\<NewFileServer>\<NewShare> /S /R:10 /W:10 /XF Meeting.Active /MT /LOG:<directory path\logname>
```

#### TIP

The /S switch copies over files, directories and subdirectories. The /XF switch skips any files that are named Meeting.Active. Current versions of the robocopy.exe with the /MT switch greatly increase copy speed by using multiple threads. For the /LOG switch, use a directory path and log file name in the form of C:\Logfiles\log.txt. This switch creates a log file of operations at the named location.

12. When the data copy is complete, in Lync Server Control Panel, click **Topology**, and then click **Status**.
13. For each server or pool where you stopped services, select the server or pool, click **Action**, and then click **Start all services**.
14. Remove the old file store from the topology and then publish the topology. For details, see [Remove a file store](#).
15. (Optional) Log on to the computer that contains the file store that you just removed as a member of the local Administrators group or the Domain Admins group, and then remove the old file share and directory.

## See also

[Reassign a Server to a Different File Store](#)

[Remove a file store](#)

# Disable TLS 1.0/1.1 in Skype for Business Server 2015

12/10/2019 • 16 minutes to read

The purpose of this article is to provide the necessary guidance for you to prepare for and implement disabling TLS 1.0 and 1.1 in your environments. This process requires extensive planning and preparation. Please carefully review all of the information in this article as you make your plan to disable TLS 1.0 and 1.1 for your organization. Note that there are many external dependencies and connectivity conditions that could be impacted by disabling TLS 1.0/1.1, so extensive planning and testing is warranted.

## In this article

- [Background and scope](#)
- [Prerequisites and process](#)
- [Advanced deployment scenarios](#)

## Background

The primary drivers for providing TLS 1.0 and 1.1 disable support for Skype for Business Server On-Premises are Payment Card Industry (PCI) Security Standards Council and Federal Information Processing Standards requirements. More information for PCI requirements can be found [here](#). Microsoft cannot provide guidance on whether or not your organization is required to adhere to these or other requirements. You must determine if it is required for you to disable TLS 1.0 and/or 1.1 in your environments.

Microsoft has produced a white paper on TLS available [here](#), and we also recommend the background reading available in this [Exchange blog](#).

## Supportability Scope

*Scope* refers to supportability boundaries. *Fully tested and supported* means we fully support and have tested disabling of TLS 1.0 and 1.1 for the listed product versions. *Currently being investigated* means just that; we are actively investigating bringing these products into scope for TLS disable support. *Out of scope* means these product versions do not support disabling TLS 1.0 or 1.1 and will not work, with noted exceptions.

### Fully tested and supported servers

- Skype for Business Server 2019 CU1 17.0.2046.123 (June 2019) or higher
- Skype for Business Server 2015 CU9 6.0.9319.548 (May 2019) or higher on Windows Server 2012 (with KB [3140245](#) or superseding update), 2012 R2 or 2016.
- In-place Upgraded Skype for Business Server 2015, with CU9 6.0.9319.548 (May 2019) or higher on Windows Server 2008 R2, 2012 (with KB [3140245](#) or superseding update), or 2012 R2.
- Exchange Connectivity and Outlook Web App with Exchange Server 2010 SP3 RU19 or higher, guidance [here](#)
- Survivable Branch Appliance (SBA) with Skype for Business Server 2015 CU6 HF2 or higher (confirm with your vendor that they packaged the appropriate updates and have been made available for your appliance)
- Survivable Branch Server (SBS) with Skype for Business Server 2015 CU6 HF2 or higher
- Lync Server 2013 **Edge Role Only**, this is because Edge role does not have a dependency on Windows Fabric 1.0.

### Fully tested and supported clients

- Lync 2013 (Skype for Business) Desktop Client, MSI and C2R, including Basic [15.0.5023.1000](#) or higher
- Skype for Business 2016 Desktop Client, MSI [16.0.4678.1000](#) or higher, including Basic

- Skype for Business 2016 Click to Run Require the [April 2018](#) Updates:
  - Monthly and Semi-Annual Targeted, 16.0.9126.2152 or higher
  - Semi-Annual and Deferred Channel, 16.0.8431.2242 or higher
- Skype for Business on Mac 16.15 or higher
- Skype for Business for iOS and Android 6.19 or higher
- Microsoft Teams Rooms (previously known as Skype Room System V2 SRS V2) 4.0.64.0 (December 2018) or higher
- Surface Hub update for Team edition based on KB4499162 (May 2019, OS Build 15063.1835) or higher
- Skype Web App 2015 CU6 HF2 or higher (ships with Server)

### Currently being investigated

- Call Quality Dashboard (new install after TLS 1.0, 1.1 have been disabled, see below)\*

### Out of scope

Except where noted, the following products are not in scope for TLS 1.0/1.1 disable support and will not function in an environment where TLS 1.0 and 1.1 have been disabled. What this means: if you still utilize out-of-scope servers or clients, you must update or remove these if you need to disable TLS 1.0/1.1 anywhere in your Skype for Business Server on-premises deployment.

- Lync Server 2013
- Lync Server 2010
- Windows Server 2008 or lower
- Lync for Mac 2011
- Lync 2013 for Mobile - iOS, iPad, Android or Windows Phone
- Lync "MX" Windows Store client
- Lync Room System (a.k.a. SRSv1). LRS reached end of support on October 9, 2018 and will not be updated to support TLS 1.2.
- All Lync 2010 clients
- Lync Phone Edition - updated guidance [here](#).
- 2013 based Survivable Branch Appliance (SBA) or Survivable Branch Server (SBS)
- Cloud Connector Edition (CCE)
- Skype for Business for Windows Phone

### Exceptions

#### Lync Server 2013

Lync Server 2013 takes a dependency on Windows Fabric version 1.0. In the design phase for Lync Server 2013, Windows Fabric 1.0 was chosen for its compelling and new distributed architecture to provide replication, high availability, and fault tolerance. Over time, both Skype for Business Server and Windows Fabric have greatly improved this joint architecture with significant re-design in subsequent versions. Current Skype for Business 2015 Server uses Windows Fabric 3.0, for example.

Unfortunately, Windows Fabric 1.0 **does not support TLS 1.2. However, we will be updating Lync Server 2013 to work with TLS 1.2.** This will be coming in the next Cumulative Update for Lync Server 2013. We're providing TLS 1.2 support to enable co-existence, migration, federation, and hybrid scenarios.

If your organization is required to disable TLS 1.0 and 1.1, and you currently use Lync Server 2013, we recommend you begin your planning process, with the possibility you may have to In-place upgrade or Side-by-Side migrate (new pools, move users) to Skype for Business Server 2015 or higher. Or you may want to accelerate migration to Skype for Business Online.

#### Call Quality Dashboard

On-Premises Call Quality Dashboard currently has a dependency on TLS 1.0 during new install (first time

installing into your On-Premises environments). We are currently investigating this issue and plan to release a fix in the near future. If you are planning to install CQD and also disable TLS 1.0, we recommend that you complete CQD installation first, and then proceed with TLS 1.0 disabling.

#### **Third-party devices**

On third-party devices such as 3PIP phones, Video conferencing, Reverse Proxies and Load Balancers, be sure to validate TLS 1.2 supportability, test carefully, and contact the vendor if needed.

#### **Federation considerations when disabling TLS 1.0/1.1 on Edge servers**

You must carefully plan for and consider the impact of disabling TLS 1.0/1.1 on your Edge servers. Once TLS 1.0 and 1.1 are disabled, you may find that other organizations are no longer be able to federate with your organization.

You may opt to keep TLS 1.0/1.1 enabled on your Edge servers to maintain backward compatibility with non-patched (SfB 2015, Lync 2013) or older (2010) external systems.

Microsoft cannot provide advice or recommendations on whether or not your Edge network (or any network) falls under PCI standard; that must be determined by the individual company.

Skype for Business Online is capable of TLS 1.2 today, so no impact to Hybrid/Federation with Online is expected.

PIC (Public IM Connectivity) to Skype Consumer service: We do not expect disabling TLS 1.0/1.1 to impact [Skype Connectivity](#); Microsoft PIC Gateways are already TLS 1.2 capable.

## **Prerequisites and process**

Except where noted above, once TLS 1.0 and 1.1 are disabled out-of-scope servers, clients and devices will longer function properly, or at all. This may mean you need to pause and wait for updated guidance from Microsoft. Once you are satisfied that you meet all requirements and have a plan to address gaps, proceed.

At a high level, while Skype for Business Server 2019 is ready for procedure at install, Skype for Business Server 2015 will require that you install CU9, applying pre-requisite updates to .NET and SQL, deploying prerequisite registry keys, and finally a separate round of OS configuration updates (i.e. disabling TLS 1.0 and 1.1 via registry file import). It is critically important that you complete installation of all prerequisites, including Skype for Business Server 2015 CU6 HF2, prior to disabling TLS 1.0 and 1.1 on any server in your environment. Every Skype for Business server, including Edge role and SQL Backends, requires the updates. Also ensure that all supported (in-scope) clients have been updated to the required minimum versions. Don't forget to update management workstations as well.

We want to follow the usual order of operations of "inside out" for upgrading Skype for Business servers. Treat Director pools, Persistent chat, and Paired Pools in the same manner you normally would. Order and methods for upgrade are covered [here](#) and [here](#).

#### **High-level process**

1. Test all steps in your lab prior to configuring production servers.
2. Back up and preserve a copy of exported registry on each and every individual server to be updated. You cannot share registries between servers; they contain unique machine-based keys.
3. Upgrade all Skype for Business 2015 servers to CU9 or higher. For Skype for Business Server 2019, upgrade to CU1 or higher.
4. Install all prerequisites to all servers.
5. Deploy prerequisite registry keys.
6. Ensure that all in-scope clients are updated.
7. Disable TLS 1.0 and 1.1 via registry import.
8. Validate that workloads are functioning as expected.
  - If problems are encountered, troubleshoot and resolve, or

- Restore registry from step 2 to re-enable TLS 1.0 and 1.1
9. Validate that only TLS 1.2 is being used.

### Install prerequisites to all servers

Extensive dependency updating is required before you begin to disable TLS 1.0 and 1.1 at the operating system level in your Skype for Business Server 2015 deployments. The following are the minimum versions that can support TLS 1.2. Deploy all prerequisite updates across every Skype for Business server in your environment before you begin disabling TLS 1.0 and 1.1.

- Skype for Business Server 2015 CU9 6.0.9319.548 (May 2019) or higher
- [.NET Framework 4.7](#) or higher with SchUseStrongCrypto enabled in the registry (provided below)
- SQL must be updated on all Skype for Business 2015 servers and backends. Update Enterprise Edition Pool SQL Backends first, then their respective FEs.
  - [SQL Server 2014 SP1 + CU5](#), or higher / SQL Server 2012 SP2 + CU16 or higher / [SQL Server 2014 RTM + CU12](#), or higher / SQL Server 2014 SP2
  - [SQL Server Native Client for SQL Server 2012](#)
  - [Microsoft ODBC Driver 11 for SQL Server](#), or higher
  - [Shared Management Objects for SQL Server 2014 SP2](#)
  - [SQLSysClrTypes for SQL server 2014 SP2](#)

### Basic steps to install pre-requisites, in recommended order of operations

1. Install the Skype for Business Server CU9 update to all servers.
  - a. Install the update to components using the updater.
  - b. Update databases according to documented procedures. For Skype for Business Server 2015, see KB [3061064](#).
  - c. Validate product functionality in the deployment prior to moving forward with any other changes.
2. Download .NET 4.7 Offline Installer.
  - a. Reference: <https://www.microsoft.com/download/details.aspx?id=55167>
  - b. Ensure that Skype for Business Server 2015 services are stopped on the Front End server.
  - c. Reference: <https://support.microsoft.com/help/3061064/updates-for-skype-for-business-server-2015>
  - d. Ex (Standard Edition): `Stop-CsWindowsService`
  - e. Ex (Enterprise Edition): `Invoke-CsComputerFailover`
  - f. Run the installer package.
  - g. Reboot the server.
3. Update SQL Express 2014 on all servers.
  - a. Reference: <https://support.microsoft.com/help/3135244/tls-1-2-support-for-microsoft-sql-server>
  - b. Download SQL 2014 SP2
    - Reference: <https://www.microsoft.com/download/details.aspx?id=53168>
  - c. Copy the installation media to a folder on the server (Ex: C:\01\_2014SqlSp2)
  - d. Ensure Skype for Business Server 2015 services are stopped on the Front End server
    - Ex (Standard Edition): `Stop-CsWindowsService`
    - Ex (Enterprise Edition): `Invoke-CsComputerFailover`
  - e. Open an Admin Command Prompt, and upgrade all installed components and instances
    - Example: `C:\01_2014SqlSp2\SQLServer2014SP2-KB3171021-x64-ENU.exe /qs /IAcceptSQLServerLicenseTerms /Action=Patch /AllInstances`
4. Update SQL Native Client.
  - a. Reference: <https://support.microsoft.com/help/3135244/tls-1-2-support-for-microsoft-sql-server>.
  - b. Download from <https://www.microsoft.com/download/details.aspx?id=50402>
  - c. Ensure Skype for Business Server 2015 services are stopped on the Front End server.

- Ex (Standard Edition): `Stop-CsWindowsServices`
  - Ex (Enterprise Edition): `Invoke-CsComputerFailover`
- d. Stop the SQL instances installed from running
- Ex: `Get-Service 'MSSQL$RTCLocal' | Stop-Service`
  - Ex: `Get-Service 'MSSQL$LYNCLOCAL' | Stop-Service`
  - Ex (Standard Edition Only): `Get-Service 'MSSQL$RTC' | Stop-Service`
- e. Install the update.
5. Update ODBC Driver 11 for SQL Server to include support for TLS 1.2 (KB [3135244](#)).
- a. Download [ODBC Driver 11 for SQL Server - Windows](#).
  - b. Ensure that Skype for Business Server 2015 services are stopped on the Front End server.
    - Example (Standard Edition): `Stop-CsWindowsService`
    - Example (Enterprise Edition): `Invoke-CsComputerFailover`
  - c. Install the update.
6. Deploy prerequisite registry keys.

### Pre-requisite registry keys

Copy/paste the following text into Notepad and rename TLSPreReq.reg or a name of your choice, then import:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]

"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]

"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]

"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]

"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]

"DefaultSecureProtocols"=dword:00000AA0

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]

"DefaultSecureProtocols"=dword:00000AA0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000001
```

For SQL back ends for Enterprise Edition Pools, prerequisites and TLS disable should be treated as any SQL or OS

updates would; refer to: <https://docs.microsoft.com/skypeforbusiness/manage/topology/patch-or-update-a-back-end-or-standard-edition-server>

While both the prerequisite application and TLS disabling steps can be combined, we strongly recommend all prerequisites be applied before proceeding with disabling of TLS 1.0 and 1.1 at the operating system level. The best practice approach would be to prepare the environment by deploying all prerequisites, validating that workloads all function correctly and as expected, and then proceeding with TLS 1.0/1.1 disable at a later time.

### Disable TLS 1.0 and 1.1 via registry import

Before you proceed with the next steps, *make sure you have completed all prerequisites and updated Skype for Business Servers.*

Copy the following text into a Notepad file and rename it **TLSDisable.reg**:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002]
```

```
"Functions"="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]
```

```
"AllowInsecureRenegoClients"=dword:00000000
```

```
"AllowInsecureRenegoServers"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES_128/128]
```

```
"Enabled"=dword:FFFFFFFF
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES_256/256]
```

```
"Enabled"=dword:FFFFFFFF
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES_56/56]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2_128/128]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2_40/128]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2_56/128]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2_56/56]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4_128/128]
```



"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_40/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_56/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4\_64/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]

"Enabled"=dword:FFFFFFFF

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Client]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol

Unified Hello\Server]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Client]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]

"DisabledByDefault"=dword:00000001

"Enabled"=dword:00000000
```

Import the .reg file on each server you wish to disable TLS 1.0 and 1.1. Reboot the server. Once the services have come back online, move to the next server. The approach for Enterprise Edition Pools is the same you would take for any OS update.

You may have noticed we are doing more than just disabling TLS 1.0 and 1.1 here. We are supporting Cipher Suite re-order (as shown above) and the disabling of some older weak ciphers. This is the first time we have officially supported these changes to SCHANNEL and Crypto API on Skype for Business Server, and it is important to note that these changes are the only ones we support and have tested at this time. We may consider additional configurations in the future, but for now, please do not modify the registry import file in your implementation.

### Validate that workloads are functioning as expected

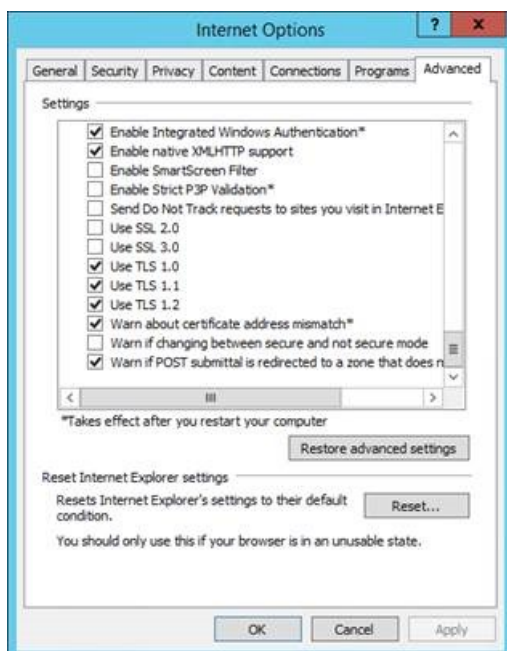
Once TLS 1.0 and 1.1 have been disabled in your environment, ensure that all your main workloads are functioning as expected, such as IM & Presence, P2P calls, Enterprise Voice, etc.

### Validate only TLS 1.2 is being used

Have your Security Team perform a new audit of Skype for Business traffic to ensure that the older protocols TLS 1.0 and 1.1 are no longer in use.

Alternatively, you can use Internet Explorer to test TLS connections to web services from Skype for Business Server 2015 after TLS 1.0 and TLS 1.1 have been disabled.

1. Launch Internet Explorer.
2. Select **Tools > Internet Options**.
3. Select the **Advanced** tab.
4. Under **Settings**, scroll to the bottom.
5. Verify that TLS 1.0, TLS 1.1, and TLS 1.2 are enabled.
6. Browse the Internal Web Service URL of your Sfb 2015 pool (should connect successfully).
7. Go back into Internet Explorer and disable the option to **Use TLS 1.2** only.
8. Browse the Internal Web Service URL of your Sfb 2015 pool again (should fail to connect).



# Advanced deployment scenarios

Because some dependency prerequisites are required to support TLS 1.2 in Skype for Business Server 2015, installing from RTM media will fail on any system where TLS 1.0 and 1.1 have been disabled.

## Deploying New Standard Edition Servers or Enterprise Edition Pools once TLS 1.0 and 1.1 have been disabled in your environment.

**Option 1:** Use [SmartSetup](#). Note that we are updating SmartSetup to accommodate the updated SQL binaries in a future CU, and will update this article in the future.

**Option 2:** Pre-install local SQL instances (RTCLOCAL and LYNCLOCAL)

1. Download and copy SQL Express 2014 SP2 (SQLEXP\_x64.exe) to local folder on FE. Let's say folder path <SQL\_FOLDER\_PATH>.
2. Launch PowerShell or Command Prompt and navigate to <SQL\_FOLDER\_PATH>.
3. Create the RTCLOCAL SQL instance by running the command below. Wait until SQLEXP\_x64.exe finishes before proceeding:

```
SQLEXP_x64.exe /Q /IACCEPTSQLSERVERLICENSETERMS /UPDATEENABLED=0 /HIDECONSOLE /ACTION=Install /FEATURES=SQLEngine,Tools /INSTANCENAME=RTCLOCAL /TCPENABLED=1 /SQLSVCAccount="NT AUTHORITY\NetworkService" /SQLSYSADMINACCOUNTS="Builtin\Administrators" /BROWSERSVCSTARTUPTYPE="Automatic" /AGTSSVCAccount="NTAUTHORITY\NetworkService" /SQLSVCSTARTUPTYPE=Automatic
```

4. Create the LYNCLOCAL SQL instance by running the command below. Wait until SQLEXP\_x64.exe finishes before proceeding to the next step:

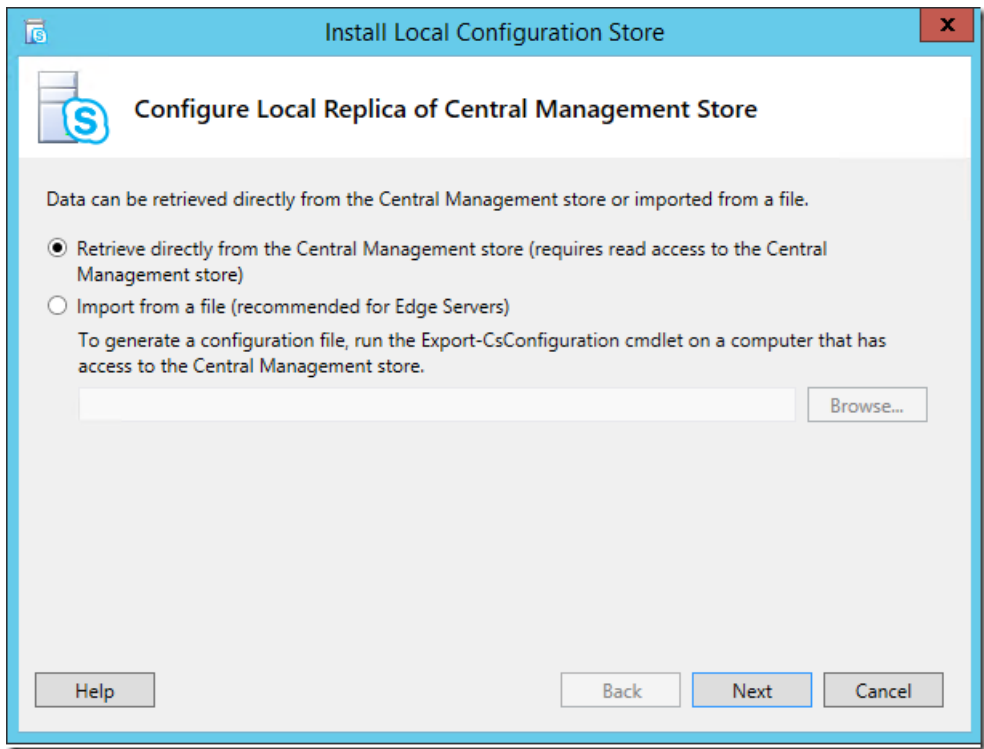
```
SQLEXP_x64.exe /Q /IACCEPTSQLSERVERLICENSETERMS /UPDATEENABLED=0 /HIDECONSOLE /ACTION=Install /FEATURES=SQLEngine,Tools /INSTANCENAME=LYNCLOCAL /TCPENABLED=1 /SQLSVCAccount="NT AUTHORITY\NetworkService" /SQLSYSADMINACCOUNTS="Builtin\Administrators" /BROWSERSVCSTARTUPTYPE="Automatic" /AGTSSVCAccount="NTAUTHORITY\NetworkService" /SQLSVCSTARTUPTYPE=Automatic
```

5. Run Skype for Business Server 2015 RTM setup.
6. Follow the remaining steps from the prerequisites section above.

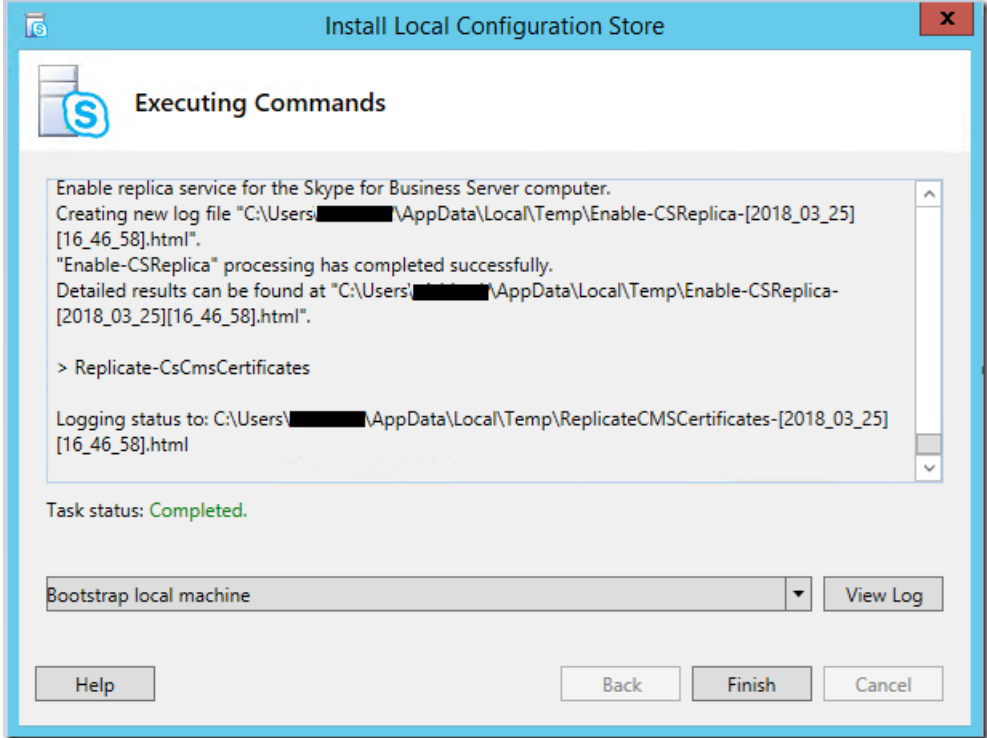
**Option 3:** You may also manually replace binaries in a local installation media directory as follows:

1. [Install prerequisites for Skype for Business Server](#)
2. Install .NET 4.7:
  - **Note:** We first introduced support for .NET 4.7 in Skype for Business Server 2015 CU5 (6.0.9319.281). Therefore, in later steps below we will be updating Core Components prior to the main install.
  - Download: <https://www.microsoft.com/download/details.aspx?id=55167>.
  - Reference: [Software that should be installed before a Skype for Business Server 2015 deployment](#)
3. Copy ISO Files/Folders:
  - With the Skype for Business Server 2015 ISO attached, open the root directory of the drive it is attached as (Ex: D:) in File Explorer.
  - Copy all folders and files to a folder on a local disk (Ex: C:\SkypeForBusiness2015ISO).
  - **Note:** Prior to installing components, some files will need to be updated for support of TLS 1.2.
4. Replace MSI/EXE Packages:
  - Replace the existing MSI and EXE packages in the /Setup/amd64/ folder of the installation media on the local machine.

- SQL 2014 SP2 Express: <https://www.microsoft.com/en-us/download/details.aspx?id=53167>
    - Rename to SQLEXPRESS\_x64 on the local machine, and replace the existing file in the Setup/amd64/ folder of the installation media.
  - SQL Native Client: <https://www.microsoft.com/en-us/download/details.aspx?id=50402>
    - **Note:** Rename this if necessary to sqlncli.msi, and then replace the existing file that exists in the Setup/amd64/ folder of the installation media.
  - SQL Management Objects: <https://www.microsoft.com/en-us/download/details.aspx?id=53164>
    - **Note:** The Feature pack will have a lot of items that can be downloaded. Select to download SharedManagementObjects.msi only.
    - **Note:** Replace the existing file that exists in the Setup/amd64/ folder of the installation media.
  - SQL CLR Types: <https://www.microsoft.com/en-us/download/details.aspx?id=53164>
    - **Note:** The Feature pack will have a lot of items that can be downloaded. Select to download CQLSysClrTypes.msi only
    - **Note:** Replace the existing file that exists in the Setup/amd64/ folder of the installation media.
5. Install Core Components:
- Run Setup.exe from the Setup/amd64/ folder of the installation media. Follow the instructions to install Core Components
  - Close Core Components.
6. Update Core Components:
- Download the Skype for Business Update Installer.
  - Run the installer to update Core Components and install the performance counters.
  - **Note:** As of the release of CU6HF2, the auto-update feature currently only will install up to CU6. Therefore, the updater must be run separately to update Core Components to 6.0.9319.516.
  - Reference: <https://support.microsoft.com/en-us/help/3061064/updates-for-skype-for-business-server-2015>
7. Install Administrative Tools (Optional):
- This will install the Microsoft SQL Server 2012 Native Client, SQL Server 2014 Management Objects (x64), and Microsoft System CLR Types for SQL Server 2014 (x64) using the updated files. Additionally, the Skype for Business Server 2015 Topology Builder and Control Panel will be available on the local machine.
8. Install Local Configuration Store (Step 1):
- Open the Deployment Wizard, click Install or Update Skype for Business Server System, and click on **Run** at Step 1: Install Local Configuration Store.
  - Click **Next** in the **Install Local Configuration Store** dialog box.

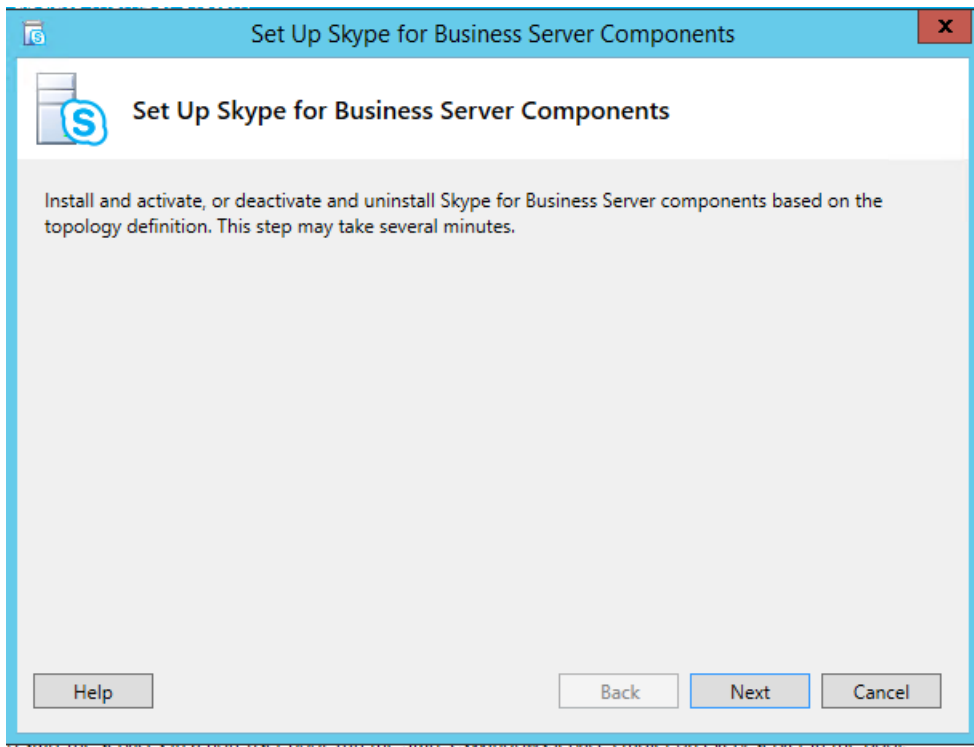


- Review the results, and ensure that the Task Status is Completed. Review the resulting log file by clicking



**View Log.**

- Click **Finish**.
9. Set up or remove Skype for Business Server Components (Step 2):
- Open the Deployment Wizard, click **Install or Update Skype for Business Server System**, and click **Run** at Step 2: Set up or Remove Skype for Business Server Components
  - Click **Next** in the Set Up Skype for Business Server Components dialog box.



- Review the log using View Log, and validate that setup completed without issues.
  - Click **Finish**.
10. Proceed with additional installation and configuration as required (you can resume normal installation procedures at this point).

# Manage health and monitoring in Skype for Business Server

6/25/2019 • 2 minutes to read

**Summary:** Learn about monitoring and health configuration tasks in Skype for Business Server.

Topics in this section provide step-by-step procedures for monitoring and health configuration tasks you can perform in Skype for Business Server Control Panel and Skype for Business Server Management Shell.

## In this section

- [Call detail recording \(CDR\) in Skype for Business Server](#)
- [Quality of Experience \(QoE\) in Skype for Business Server](#)
- [Monitor mobility for performance in Skype for Business Server](#)
- [Using Monitoring Reports in Skype for Business Server](#)

## See also

[Plan for monitoring](#)

[Deploy monitoring](#)



# Access monitoring data in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the monitoring data used in Skype for Business Server.

Monitoring data is stored in a pair of SQL Server databases: LcsCdr for call detail recording data, and QoEMetrics for Quality of Experience data. There is nothing special about these two databases; that means that the data stored in those databases can be accessed using any of the tools you typically use for accessing and analyzing SQL Server data.

One tool you should consider for accessing and analyzing monitoring data is the Skype for Business Server Monitoring Reports. Monitoring Reports are a set of standard reports that are published by Microsoft SQL Server Reporting Service. These reports, which are accessible by using a web browser, provide usage, call diagnostic information, and media quality information, all based on call detail recording (CDR) and Quality of Experience (QoE) records stored in the CDR and QoE databases. Monitoring Reports ship with Skype for Business Server and can be installed from the Skype for Business Server Deployment Wizard after Skype for Business Server has been installed and monitoring has been configured.

As noted, Monitoring Reports requires the use of SQL Server Reporting Service. SQL Server Reporting Service can be installed at the same time you install SQL Server or can be installed any time after SQL Server itself has been installed.

For more information, see the topic [Install Monitoring Reports in Skype for Business Server](#).

# Call detail recording (CDR) in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Call detail recording (CDR) records used in Skype for Business Server.

Call detail recording (CDR) records usage and diagnostic information about peer-to-peer activities, including instance messaging, Voice over Internet Protocol (VoIP) calls, application sharing, file transfer, and meetings. The usage data can be used to calculate return on investment (ROI) and the diagnostic data can be used to troubleshoot peer-to-peer activities and meetings. When you install Skype for Business Server, you will also install a predefined collection of global configuration settings for CDR. Use the topics in this section to configure CDR.

## In this section

- [View CDR configuration information in Skype for Business Server](#)
- [Enable call detail recording in Skype for Business Server](#)
- [Create or modify a collection of CDR configuration settings in Skype for Business Server](#)
- [Delete an existing collection of CDR configuration settings in Skype for Business Server](#)
- [Manually purge the call detail recording and Quality of Experience databases in Skype for Business Server](#)

## See also

[Configure call detail recording and Quality of Experience settings in Skype for Business Server](#)

# View CDR configuration information in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to use Call Detail Recording (CDR) in Skype for Business Server.

Call Detail Recording (CDR) enables you to track usage of such things as peer-to-peer instant messaging sessions, Voice over Internet Protocol (VoIP) phone calls, and conferencing calls. This usage data includes information about who called whom, when they called, and how long they talked.

When you install Skype for Business Server, a single, global collection of CDR configuration settings is created for you. Administrators also have the option of creating custom setting collections that can be applied to individual sites. You can view the CDR configuration settings in use in your organization by using Skype for Business Server Control Panel or the [Get-CsCdrConfiguration](#) cmdlet.

## To view CDR configuration information by using Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel click **Monitoring and Archiving**.
2. A list of all your CDR configuration settings will be displayed in the **Call Detail Recording** tab; for each collection of settings you will see the collection **Name**; whether or not CDR has been enabled (the **CDR** property); and whether or not purging has been enabled (the **CDR purging** property). To see detailed information about a collection, double-click the collection, or select the appropriate collection, click **Edit**, and then click **Show Details**. Note that you can only view detailed information for a single collection of CDR configuration settings at a time.

## Viewing CDR configuration information by using Windows PowerShell cmdlets

You can view CDR configuration settings by using Windows PowerShell and the `Get-CsCdrConfiguration` cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To view CDR configuration information

- To view information about all your CDR configuration settings, type the following command in the Skype for Business Server Management Shell and then press ENTER:

```
Get-CsCdrConfiguration
```

That will return information similar to this:

```
Identity           : Global
EnableCDR          : True
EnablePurging      : True
KeepCallDetailForDays : 90
KeepErrorReportForDays : 60
PurgeHourOfDay     : 2
```

For more information, see the help topic for the [Get-CsCdrConfiguration](#) cmdlet.

# Enable call detail recording in Skype for Business Server

9/5/2019 • 2 minutes to read

**Summary:** Learn how to enable Call detail recording (CDR) records in Skype for Business Server.

Call detail recording (CDR) records usage and diagnostic information about peer-to-peer activities including instance messaging, Voice over Internet Protocol (VoIP) calls, application sharing, file transfer, and meetings. The usage data can be used to calculate return on investment (ROI) and the diagnostic data can be used to troubleshoot peer-to-peer activities and meetings.

Use the following procedure to enable CDR for your whole organization or each site in your organization.

## NOTE

In order to enable CDR you must configure monitoring and a monitoring database. For details, see [Deploying Monitoring](#).

## To enable CDR with Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Call Detail Recording**.
4. On the **Call Detail Recording** page, click the appropriate site from the table, click **Action**, and then click **Enable CDR**.

## NOTE

CDR is enabled by default.

## Enabling CDR by using Windows PowerShell cmdlets

You can enable CDR by using Windows PowerShell and the **Set-CsCdrConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To enable CDR for a single location

To disable CDR, set the EnableCDR parameter to True (\$True).

```
Set-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $True
```

### To disable CDR for a single location

To disable CDR, set the EnableCDR parameter to False (\$False). Disabling CDR does not uninstall monitoring. It

pauses the collection and storage of CDR data.

```
Set-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $False
```

### To use a single command to enable CDR in multiple locations

This command enables CDR for all the CDR configuration settings currently in use in your organization.

```
Get-CsCdrConfiguration | Set-CsCdrConfiguration -EnableCDR $True
```

For more information, see the help topic for the [Set-CsCdrConfiguration](#) cmdlet.

## See also

[Planning for Monitoring](#)

[Deploying Monitoring](#)

# Specify retention of CDR data in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage call detail recording (CDR) data for Skype for Business Server.

By default, call detail recording (CDR) data is purged after 60 days. You can use the settings on the **Call Detail Recording** page to retain the data for a longer or shorter period of time. If you disable CDR, data that was captured before CDR was enabled will also be subject to purging.

## NOTE

You should configure CDR and Quality of Experience (QoE) to retain data for the same number of days. Each call in the call detail reports (CDRs), available from the Monitoring Server Reports webpage, includes CDR and QoE information. If the purging duration for CDR and QoE is different, some calls might only include CDR data, while other may only include QoE data.

Use the following procedures to configure purge settings for CDR data.

## To specify retention of CDR data

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Call Detail Recording**.
4. On the **Call Detail Recording** page, click the appropriate site in the table, click **Edit**, and then click **Show Details**.
5. To turn on purging, select **Enable purging of CDRs**.
6. In **Keep CDRs for maximum duration (days)**: select the maximum number of days that call detail recordings should be retained.
7. In **Keep error report data for maximum duration (days)**: select the maximum number of days that error reports should be retained.
8. Click **Commit**.

## Specifying CDR retention by using Windows PowerShell cmdlets

You can create CDR retention settings by using Windows PowerShell and the Set-CsCdrConfiguration cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

## To specify CDR retention for a specific location

- This command enables purging of CDR data for the Redmond site, and configures the site to maintain both

CDR data and error reports data for 20 days.

```
Set-CsCdrConfiguration -Identity "site:Redmond" -EnablePurging -KeepCallDetailForDays 20 -  
KeepErrorReportForDays 20
```

### To specify CDR retention for multiple locations

- This command configures CDR retention for all the CDR configuration settings in use in an organization.

```
Get-CsCdrConfiguration | Set-CsCdrConfiguration-EnablePurging -KeepCallDetailForDays 20 -  
KeepErrorReportForDays 20
```

For more information, see the help topic for the [Set-CsCdrConfiguration](#) cmdlet.

## See also

[Call detail recording \(CDR\) in Skype for Business Server](#)



# Create or modify a collection of CDR configuration settings in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about Call detail recording (CDR) in Skype for Business Server.

Call detail recording (CDR) enables you to track usage of such things as peer-to-peer instant messaging sessions, Voice over Internet Protocol (VoIP) phone calls, and conferencing calls. This usage data includes information about who called whom, when they called, and how long they talked.

When you install Skype for Business Server a single, global collection of CDR configuration settings is created for you. Administrators also have the option of creating custom settings at the site scope. Whenever these site-scoped settings are used, they take precedence over the global settings. For example, if you create site-scoped settings for the Redmond site then those settings (rather than the global settings) will be used to manage CDR in Redmond.

You can create CDR configuration settings by using either Skype for Business Server Control Panel or the [New-CsCdrConfiguration](#) cmdlet. You can use Skype for Business Server Control Panel or the [Set-CsCdrConfiguration](#) cmdlet to modify existing settings. If you are using Skype for Business Server Control Panel to create or modify settings, the following options will be available to you:

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Name	Identity	Unique identifier for the CDR configuration settings being created. These settings can only be created at the site scope.
Enable monitoring of CDRs	EnableCDR	Indicates whether or not CDR is enabled.
Enable purging of CDRs	EnablePurging	Indicates whether or not CDR records will periodically be deleted from the CDR database.
Keep CDRs for maximum duration (days)	KeepCallDetailForDays	Indicates the number of days that CDR records will be kept in the CDR database. Any records older than the specified number of days will automatically be deleted. (Note that purging will take only place if purging has been enabled.)
Keep error report data for maximum duration (days)	KeepErrorReportForDays	Indicates the number of days that CDR error reports are kept. Any reports older than the specified number of days will automatically be deleted. CDR error reports are diagnostic reports uploaded by client applications.

#### NOTE

The `New-CsCdrConfiguration` and `Set-CsCdrConfiguration` cmdlets include additional options not available in Skype for Business Server Control Panel. See the [New-CsCdrConfiguration](#) and the [Set-CsCdrConfiguration](#) help topics for more information.

#### To create CDR configuration settings by using Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel click **Monitoring and Archiving**.
2. On the **Call Detail Recording** tab, click **New**.
3. In the **Select a Site** dialog box, select the site where the new configuration settings are to be created. If the dialog box is empty, that means all of your sites have already been assigned a collection of CDR configuration settings. Each site is limited to a single such collection. In that case you can either delete and then re-create the settings, or simply modify the existing settings.
4. In the **New Call Detail Recording (CDR) Setting** dialog, make the desired selections and then click **Commit**.

#### To modify existing CDR configuration settings by using Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel click **Monitoring and Archiving**.
2. Double-click the collection of settings to be modified, or select the collection, click **Edit**, and then click **Show Details**. Note that you can only modify a single collection at a time. To make the same changes to multiple collections, use the Skype for Business Server Management Shell instead.
3. In the **Edit Call Detail Recording (CDR) Setting** dialog, make the desired selections and then click **Commit**.

## Creating CDR configuration settings by using Windows PowerShell Cmdlets

You can create CDR configuration settings can also be created by using Windows PowerShell and the **New-CsCdrConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

#### To create a new collection of CDR configuration settings

This command creates a new collection of CDR configuration settings applied to the Redmond site:

```
New-CsCdrConfiguration -Identity "site:Redmond"
```

#### To create a collection of CDR configuration settings that disable call detail recording

Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties. To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of Call Detail configuration settings that, by default, allow disable Call Detail recording use a command like this:

```
New-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $False
```

#### To specify multiple property values when creating a new collection of CDR configuration settings

You can modify multiple property values by including multiple parameters. For example, this command configures the new settings to keep Call Detail records for 30 days and error reports for 90 days:

```
New-CsCdrConfiguration -Identity "site:Redmond" -KeepCallDetailForDays 30 -KeepErrorReportForDays 90
```

For more information, see the help topic for the [New-CsCdrConfiguration](#) cmdlet.

# Delete an existing collection of CDR configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to remove CDR configuration settings in Skype for Business Server.

Call Detail Recording (CDR) enables you to track usage of such things as peer-to-peer instant messaging sessions, Voice over Internet Protocol (VoIP) phone calls, and conferencing calls. This usage data includes information about who called whom, when they called, and how long they talked.

When you install Skype for Business Server, a single, global collection of CDR configuration settings is created for you. Administrators also have the option of creating custom setting collections that can be applied to individual sites. By design, settings configured at the site scope take precedence over settings configured at the global scope. If you delete site-scoped settings, then CDR will be managed in that site by using the global settings.

Note that you can also "delete" the global settings. However, the global settings will not actually be removed. Instead, all the properties in that collection will be reset to their default values. For example, by default purging is enabled in a collection of CDR configuration settings. Suppose you modify the global collection so that purging is disabled. If you later delete the global settings, all the properties will be reset to their default values. In this case, that means that purging will once again be enabled.

You can remove CDR configuration settings by using the Skype for Business Server Control Panel or the [Remove-CsCdrConfiguration](#) cmdlet.

## To remove CDR configuration settings with Skype for Business Server Control Panel

1. In Skype for Business Server Control Panel, click **Monitoring and Archiving**.
2. On the **Call Detail Recording** tab, select the collection (or collections) of CDR settings to be removed. To select multiple collections, click the first collection, hold down the Ctrl key, and click additional collections.
3. Click **Edit**, and then click **Delete**.
4. In the Skype for Business Server Control Panel dialog box, click **OK**.

## Removing CDR configuration settings by using Windows PowerShell Cmdlets

You can delete call detail recording configuration settings by using Windows PowerShell and the **Remove-CsCdrConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To remove a specified collection of CDR configuration settings

This command removes the CDR configuration settings applied to the Redmond site:

```
Remove-CsCdrConfiguration -Identity "site:Redmond"
```

### To remove all the CDR configuration settings applied to the site scope

This command removes all the CDR configuration settings applied to the site scope:

```
Get-CsCdrConfiguration -Filter "site:*" | Remove-CsCdrConfiguration
```

### **To remove all the CDR configuration settings that disable call detail recording**

This command removes all the CDR configuration settings where Call Detail recording has been disabled:

```
Get-CsCdrConfiguration | Where-Object {$_.EnableCDR -eq $False} | Remove-CsCdrConfiguration
```

For more information, see the help topic for the [Remove-CsCdrConfiguration](#) cmdlet.

## See also

[Manually purge the call detail recording and Quality of Experience databases in Skype for Business Server](#)

# Quality of Experience (QoE) in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Manage Quality of Experience (QoE) in Skype for Business Server.

Quality of Experience (QoE) records numeric data that indicates the media quality and information about participants, device names, drivers, IP addresses, and endpoint types involved in calls and sessions. When you install Skype for Business Server, you will also install a predefined collection of global configuration settings for QoE. Use the topics in this section to configure QoE settings.

## In this section

- [Create Quality of Experience configuration settings in Skype for Business Server](#)
- [Enable Quality of Experience in Skype for Business Server](#)
- [Modify Quality of Experience settings in Skype for Business Server](#)
- [Delete Quality of Experience configuration settings in Skype for Business Server](#)
- [Manually purge the call detail recording and Quality of Experience databases in Skype for Business Server](#)

## See also

[Configure call detail recording and Quality of Experience settings in Skype for Business Server](#)

# Create Quality of Experience configuration settings in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn about Quality of Experience (QoE) settings in Skype for Business Server.

Quality of Experience (QoE) metrics track the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay). These metrics are stored in a database apart from other data (such as call detail records), which allows you to enable and disable QoE independent of other data recording.

When you install Skype for Business Server, a single, global collection of QoE configuration settings is created for you. Administrators also have the option of creating custom settings at the site scope. Whenever these site-scoped settings are used, they take precedence over the global settings. For example, if you create site-scoped settings for the Redmond site then those settings (rather than the global settings) will be used to manage QoE in Redmond.

QoE configuration settings can be created by using either Skype for Business Server Control Panel or the [New-CsQoEConfiguration](#) cmdlet. If you are using Skype for Business Server Control Panel to create new settings the following options will be available to you:

UI SETTING	POWERSHELL PARAMETER	DESCRIPTION
Name	Identity	Unique identifier for the settings to be created. QoE configuration settings can only be created at the site scope.
Enable monitoring of QoE data	EnableQoE	Specifies whether QoE records will be collected and saved to the monitoring database.
Enable purging of QoE data	EnablePurging	Specifies whether records will be purged after the duration defined in the <b>Keep QoE data for a maximum duration (days)</b> property has elapsed.
Keep QoE data for maximum duration (days)	KeepQoEDataForDays	Number of days QoE data will be stored before being purged from the database. This value is ignored if purging is disabled.

## NOTE

The `New-CsQoEConfiguration` cmdlet includes additional options not available in Skype for Business Server Control Panel. For more information, see the [New-CsQoEConfiguration](#) help topic.

## To create QoE configuration settings by using Skype for Business Server Control Panel

1. Log on to the computer as a member of the `RTCUniversalServerAdmins` group, or as a member of the `CsVoiceAdministrator`, `CsServerAdministrator`, or `CsAdministrator` role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control

Panel.

3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click **New**.
5. In **Select a Site**, click the site to which the policy is to be applied, and click **OK**.
6. In **New Quality of Experience Setting**, do the following:
  - Select **Enable monitoring of QoE data** to turn on monitoring.
  - Select **Enable purging of QoE data** to turn on purging.
  - In **Keep QoE for maximum duration (days)**, select the maximum number of days that QoE records should be retained.
7. Click **Commit**.

## Creating QoE Configuration Settings by Using Windows PowerShell Cmdlets

You can create QoE configuration settings by using Windows PowerShell and the `New-CsQoEConfiguration` cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To create a new collection of QoE configuration settings

This command creates a new collection of QoE configuration settings applied to the Redmond site:

```
New-CsQoEConfiguration -Identity "site:Redmond"
```

### To create a new collection of QoE configuration settings where QoE monitoring is disabled

Because no parameters (other than the mandatory `Identity` parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties. To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of Quality of Experience configuration settings that, by default, allow disable QoE recording use a command like this:

```
New-CsQoEConfiguration -Identity "site:Redmond" -EnableQoE $False
```

### To specify multiple property values when creating a new collection of QoE configuration settings

You can multiple property values by including multiple parameters. For example, this command configures the new settings to keep QoE data for 30 days and to purge old data at 3:00 AM:

```
New-CsQoEConfiguration -Identity "site:Redmond" -KeepQoEDataForDays 30 -PurgeHourOfDay 3
```

For more information, see the help topic for the [New-CsQoEConfiguration](#) cmdlet.



# Enable Quality of Experience in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** learn how to enable Quality of Experience (QoE) in Skype for Business Server.

Quality of Experience (QoE) records numeric data that indicates the media quality and information about participants, device names, drivers, IP addresses, and endpoint types involved in calls and sessions. For details, see [Planning for Monitoring](#) in the Planning documentation.

Use the following procedure to enable QoE for your whole organization or each site in your organization.

## NOTE

To enable QoE, you must first configure monitoring and a monitoring back-end database. For details, see [Deploying Monitoring](#).

## To enable QoE by using Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click the appropriate collection from the table, click **Action**, and then click **Enable QoE**.

## Enabling QoE by Using Windows PowerShell Cmdlets

You can enable QoE by using Windows PowerShell and the **Set-CsQoEConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To enable QoE for a single location

To enable QoE, set the EnableQoE parameter to True (\$True).

```
Set-CsQoEConfiguration -Identity "site:Redmond" -EnableQoE $True
```

### To disable QoE for a single location

To disable QoE, set the EnableQoE parameter to False (\$False). This does not uninstall monitoring. It pauses the collection and storage of QoE data.

```
Set-CsQoEConfiguration -Identity "site:Redmond" -EnableQoE $False
```

### To use a single command to enable QoE in multiple locations

This command enables QoE for all the QoE configuration settings currently in use in your organization.

```
Get-CsQoEConfiguration | Set-CsQoEConfiguration "site:Redmond" -EnableQoE $True
```

For details, see [Set-CsQoEConfiguration](#).

## See also

[Planning for Monitoring](#)

[Deploying Monitoring](#)

# Modify Quality of Experience settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to specify retention of QoE data in Skype for Business Server.

By default, Quality of Experience (QoE) data is purged after 60 days. You can use the settings on the **Quality of Experience Data** page to retain the data for a longer or shorter period of time. If you disable QoE, data that was captured before QoE was enabled will also be subject to purging.

## NOTE

You should configure call detail recording (CDR) and QoE to retain data for the same number of days. Each call in the call detail reports (CDRs), available from the Monitoring Reports homepage, includes CDR and QoE information. If the purging duration for CDR and QoE is different, some calls may only include CDR data, while other may only include QoE data.

The following procedure describes how to configure purge settings for QoE data.

## To specify retention of QoE data by using Skype for Business Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click the appropriate site from the table, click **Edit**, and then click **Show Details**.
5. To turn on purging, select **Enable Purging of QoE**.
6. In **Keep QoE for maximum duration (days)** select the maximum number of days that QoE data should be retained.
7. Click **Commit**.

## Specifying QoE Retention by Using Windows PowerShell Cmdlets

You can create QoE retention settings by using Windows PowerShell and the **Set-CsQoEConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To specify QoE retention for a specific location

- This command enables purging of QoE data for the Redmond site, and configures the site to maintain QoE data for 20 days.

```
Set-CsQoeConfiguration -Identity "site:Redmond" -EnablePurging -KeepQoeDataForDays 20
```

### To specify QoE retention for multiple locations

- This command configures QoE retention for all the QoE configuration settings in use in an organization.

```
Get-CsQoeConfiguration | Set-CsQoeConfiguration-EnablePurging -KeepQoeDataForDays 20
```

For more information, see the help topic for the [Set-CsQoeConfiguration](#) cmdlet.

## See also

[Deploying Monitoring](#)

# Delete Quality of Experience configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to delete Quality of Experience (QoE) settings in Skype for Business Server.

Quality of Experience (QoE) metrics track the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay). These metrics are stored in a database apart from other data (such as call detail records), which allows you to enable and disable QoE independent of other data recording.

When you install Skype for Business Server, a single, global collection of QoE configuration settings is created for you. Administrators also have the option of creating custom setting collections that can be applied to individual sites. By design, settings configured at the site scope take precedence over settings configured at the global scope. If you delete site-scoped settings, then QoE will be managed in that site by using the global settings.

Note that you can also "delete" the global settings. However, the global settings will not actually be removed. Instead, all the properties in that collection will be reset to their default values. For example, by default purging is enabled in a collection of QoE configuration settings. Suppose you modify the global collection so that purging is disabled. If you later delete the global settings, all the properties will be reset to their default values. In this case, that means that purging will once again be enabled.

You can remove QoE configuration settings by using the Skype for Business Server Control Panel or by using the [Remove-CsQoEConfiguration](#) cmdlet.

## To delete QoE configuration settings by using Skype for Business Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see **Delegate Setup Permissions**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click the policy that you want, click **Edit**, and then click **Delete**.
5. Click **OK**.

## Removing QoE Configuration Settings by Using Windows PowerShell Cmdlets

You can delete QoE configuration settings by using Windows PowerShell and the **Remove-CsQoEConfiguration** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To remove a specified collection of QoE configuration settings

This command removes the QoE configuration settings applied to the Redmond site:

```
Remove-CsQoEConfiguration -Identity "site:Redmond"
```

### To remove all of the QoE configuration settings applied to the site scope

This command removes all the QoE configuration settings applied to the site scope:

```
Get-CsQoEConfiguration -Filter "site:*" | Remove-CsQoEConfiguration
```

### To remove all of the QoE configuration settings where QoE monitoring is disabled

This command removes all the QoE configuration settings where QoE monitoring has been disabled:

```
Get-CsQoEConfiguration | Where-Object {$_.EnableQoE -eq $False} | Remove-CsQoEConfiguration
```

For details, see [Remove-CsQoEConfiguration](#).

## See also

[Manually purge the call detail recording and Quality of Experience databases in Skype for Business Server](#)

# Monitor mobility for performance in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Mobility Service (Mcs) and the Unified Communications Web API (UCWA) in Skype for Business Server.

The Skype for Business Server Mobility Service (Mcs) and the Unified Communications Web API (UCWA) increase the load on Front End Servers and Front End pools. Mobile devices that maintain a connection to the server even when the mobile application is minimized, such as Android and Nokia devices running Lync 2010 Mobile, as well as Android and Apple devices running Lync 2013 Mobile, impose a greater load than devices that terminate their connection to the server when the mobile application is minimized. As your mobility usage increases, you must monitor mobility performance to determine when you need to increase your capacity.

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

Several limits influence mobility performance:

- Available memory
- Request queue limit
- Concurrent connections
- IIS queue length

Other limits on servers that can influence mobility performance are a maximum of 12 concurrent sign-ins, authentications, session renewals, and terminations. These maximums do not need to be modified for most deployments.

## In this section

- [Monitor for server memory capacity limits in Skype for Business Server](#)
- [Monitor Mobility Service and UCWA usage in Skype for Business Server](#)
- [Configure Mobility Service for high performance in Skype for Business Server](#)
- [Monitoring IIS request tracing log files in Skype for Business Server](#)
- [Mobility performance counters in Skype for Business Server](#)

# Monitor for server memory capacity limits in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn how to monitor for server memory capacity limits in Skype for Business Server.

## Caution

The information in this topic that refers to Capacity Planning pertains only to Lync 2010 Mobile clients and the Mobility Service (Mcx). Capacity Planning for the Unified Communications Web API (UCWA), used by the Lync 2013 Mobile clients, is provided by the Lync Server 2013, Planning Tool.

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

Two mobility performance counters can help you to determine your current usage and help you plan capacity for the Skype for Business Server Mobility Service (Mcx), as well as to monitor memory usage for UCWA. For UCWA, the counter category is **LS:WEB - UCWA**. For the Mobility Service (Mcx), the counters are under the category **LS:WEB - Mobile Communication Service**. The counters to monitor are:

- **Currently Active Session Count with Active Presence Subscriptions**, which is the current number of endpoints registered through UCWA or the Mobility Service (Mcx) that have active presence subscriptions (number of always-connected mobile users)
- **Currently Active Session Count**, which is the current number of endpoints registered through UCWA or the Mobility Service

If the difference between **Currently Active Session Count with Active Presence Subscriptions** and **Currently Active Session Count** is small over time, this means that most mobile device users have an always-connected device, such as an Android or Nokia mobile device (for Mcx only). UCWA always-connected devices include Apple and Android devices running Lync 2013 Mobile clients). If **Currently Active Session Count** is much higher than **Currently Active Session Count with Active Presence Subscriptions**, this indicates that more users are using a background endpoint device, such as an Apple iOS device or Windows Phone under Mcx. (Windows Phone is the only Lync 2013 Mobile client that will register as this).

You should set a limit on the **Currently Active Session Count with Active Presence Subscriptions** and **Currently Active Session Count** performance counters based on your expected usage, capacity planning results, and ongoing monitoring of Mobility Service and other Front End Server counters. The limits you set should enable you to evaluate server capacity and raise alerts when capacity is exceeded.

To determine the appropriate limits, you need to first determine how much memory is available on the Front End Server for the Mobility Service. Monitor the counters to determine when you need to plan for extra capacity, according to the following formula:

Total memory used by the Mcx Mobility Service (MB) =  $164 + (400 + 134) / 1024 * \text{Currently Active Session Count with Active Presence Subscriptions} + 400 / 1024 * (\text{Currently Active Session Count} - \text{Currently Active Session Count with Active Presence Subscriptions})$



### IMPORTANT

The Microsoft Lync Server 2010 Capacity Calculator is a spreadsheet that is prepopulated with all of the formulas that enable a planner to determine what the requirements will be for the Skype for Business servers, including CPU, memory, and hard drive. You can [download the spreadsheet and an associated document](#).

The Front End Server needs enough available memory to support the Mobility Service in failover situations. You can monitor the current available memory on the Front End Server by using the **Memory\Available Mbytes** counter, or by using the equation mentioned earlier, to plan for the amount of memory that you expect the Mobility Service to use.

If the amount of memory available on the Front End Server is lower than 1,500 MB when you plan for the expected number of mobility users, you need to add more hardware to support the Mobility Service. For more details, see [Monitor mobility for performance in Skype for Business Server](#) in the Operations documentation.

## See also

[Monitor mobility for performance in Skype for Business Server](#)

# Monitor Mobility Service and UCWA usage in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Manage the Mobility Service (Mcx) and the Unified Communications Web API (UCWA) in Skype for Business Server.

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

On an ongoing basis, you should monitor the CPU and memory that is used by the Skype for Business Server Mobility Service (Mcx) and the Unified Communications Web API (UCWA). To monitor usage, you can use the following:

### For Unified Communications Web API (UCWA):

- The **LyncUcwa** worker process in Internet Information Services (IIS) Manager. In the **Worker Processes** pane, look at the **CPU %** and **Private Bytes (KB)** (memory) columns.
- The **CPU** and **Processor** performance counters.

For most deployments, UCWA CPU usage should be below 15 percent on average. Memory usage should fall within the limits described in [Monitor for server memory capacity limits in Skype for Business Server](#).

In addition to CPU and memory usage counters, you can use the following performance counters to help determine when a server is overloaded with requests:

- **LS:WEB - Throttling and Authentication\WEB - Total Requests in Processing**, which indicates the number of pending web requests on the server. When this counter reaches 10,000, subsequent requests will fail, with the error message, "503 - Service Unavailable."
- **ASP.NET\Requests Queued** (should always be zero).

## NOTE

If you meet or exceed these values, you should revisit and re-compute your capacity planning for the correct sizing of CPU, number of cores and memory for the computers hosting the web services.

### For the Mobility Service (Mcx):

- The **CSIntMcxAppPool** and **CSExtMcxAppPool** worker processes in Internet Information Services (IIS) Manager. In the **Worker Processes** pane, look at the **CPU %** and **Private Bytes (KB)** (memory) columns.
- The **CPU** and **Processor** performance counters.

For most deployments, Mobility Service CPU usage should be below 15 percent, on average. Memory usage should fall within the limits described in [Monitor for server memory capacity limits in Skype for Business Server](#).

In addition to CPU and memory usage counters, you can use the following ASP.NET performance counters to help

determine when a server is overloaded with requests:

- **ASP.NET v2.0.50727\Requests Current**, which indicates the number of pending web requests on the server. When this counter reaches 5,000, subsequent requests will fail with the error message, "503 - Service Unavailable."
- **ASP.NET\Requests Queued** (should always be zero).

#### NOTE

If you meet or exceed these values, you should revisit and recompute your capacity planning for the correct sizing of CPU, number of cores, and memory for the computers hosting the web services.

#### NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## See also

[Monitor for server memory capacity limits in Skype for Business Server](#)

# Configure Mobility Service for high performance in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Mobility Service in Skype for Business Server.

## **IMPORTANT**

This topic applies only to the Skype for Business Server Mobility Service (Mcs), and does not apply to Unified Communications Web API (UCWA), as delivered in the Cumulative Updates for Lync Server 2013: February 2013.

When you install the Mobility Service (Mcs) on Internet Information Services (IIS) 7.5, the Mobility Service installer configures some performance settings on the Front End Server. We recommend that you use IIS 7.5 for mobility. The settings affect the maximum number of concurrent user requests and the maximum number of threads that are allowed for the Mobility Service.

Here are the performance settings:

### **Settings for Mcs on IIS 7.5**

1. **maxConcurrentThreadsPerCPU** is set to zero (0).
2. **maxConcurrentRequestsPerCPU** is set to zero (0).
3. ASP.NET process model is set to AutoConfig (for IIS 7.5 only).
4. HTTP.sys queue limit is set to 1,000 (by default).

# Mobility performance counters in Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Learn about the performance counters that you can use to monitor servers running the Unified Communications Web API (UCWA) and the Skype for Business Server Mcx Mobility Service.

The following tables list the names and descriptions of performance counters that you can use to monitor servers running the Unified Communications Web API (UCWA) and the Skype for Business Server Mcx Mobility Service.

The category name for the counters in the UCWA table is **LS:WEB - UCWA**.

The category name for the counters in the Mcx Mobility Service table is **LS:WEB - Mobile Communication Service**.

## NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## Performance Counters for UCWA

COUNTER	DESCRIPTION
Active Application Count	The current number of applications
Active Application Sharing Modality Count	The current number of Application Sharing modality
Active Audio Modality Count	The current number of Audio modality
Active Data Collaboration Modality Count	The current number of Data Collaboration modality
Active Directory Photo Get Latency (ms)	This counter shows the average time (in milliseconds) to retrieve a photo from active directory
Active Messaging Modality Count	The current number of Messaging modality
Active Panoramic Video Modality Count	The current number of Panoramic Video modality
Active Pending Get Count	The number of currently active pending gets; long-held connections to the server
Active Session Count	The current number of endpoints registered in UCWA per application and total
Active User Instance Count	The current number of user instances
Active User Instances without Application	The current number of user instances without application

COUNTER	DESCRIPTION
Active Video Modality Count	The current number of Video modality
Application Creation Requests Received/Second	The per second rate of received application creation requests
AS MCU Join Failures	The number of AS MCU Join Failures
AV MCU Join Failures	The number of AV MCU Join Failures
Average Application Startup Time (ms)	The average application startup time in Milliseconds
Average Lifetime for Session (ms)	The average lifetime for a session in milliseconds
Data MCU Join Failures	The number of Data MCU Join Failures
Exchange Contact Search Latency (ms)	This counter shows the average time (in milliseconds) to search contact in Exchange
Exchange HD Photo Get Latency (ms)	This counter shows the average time (in milliseconds) to retrieve a photo from Exchange
HTTP 4xx Responses/Second	The per second rate of responses with HTTP 4xx code
HTTP 5xx Responses/Second	The per second rate of responses with HTTP 5xx code
IM MCU Join Failures	The number of IM MCU Join Failures
Number of Active Directory Photo Get Failures	The total number of failures to retrieve photos from Active Directory
Number of Contact Search failures	The total number of failures to search contacts in Exchange
Number of Deserialization Failures	The total number of deserialization failures
Number of HD Photo Get Failures	The total number of failures to retrieve HD photos from Exchange
Over The Maximum Subscriptions Per Application	The number of Subscription requests over the maximum allowed per application
Over The Maximum Subscriptions Per Batch	The number of Subscription requests over the maximum allowed per batch
Presence Subscription Failures	The number of failures to subscribe presence
Registering Endpoint Failures	The number of failures to register endpoints
Requests Received/Second	The per second rate of received requests
Requests Succeeded/Second	The per second rate of successful requests (HTTP 2xx/3xx response codes)

COUNTER	DESCRIPTION
Succeeded Create Application Requests/Second	The per second rate of successful application creation requests
Timed Out Pending Get Count	The number of pending gets that timed out
Total Application Creation Requests Received	The total number of application creation requests received since the service was started
Total HTTP 4xx Responses	The total number of HTTP 4xx responses
Total HTTP 5xx Responses	The total number of HTTP 5xx responses
Total Requests Received on the Command Channel	The total number of requests received on the command channel
Total Requests Succeeded	The total number of requests that succeeded
Total Sessions Initiated	The total number of sessions that were initiated since the service was started
Total Sessions Terminated Because of Idle Timeout	The total number of sessions that were terminated because of user idle timeout
Total Throttled Applications	The number of throttled applications

### Performance Counters for Mcx Mobility Service

COUNTER	DESCRIPTION
Average Lifetime for a Session in Milliseconds	The average lifetime for a session in milliseconds
Current Push Notification Subscriptions	The current number of push notification subscriptions. This number, in conjunction with Currently Active Session Count, represents the subset of currently active sessions that are registered for Windows Mobile or iPhone devices.
Currently Active Network Timeout Poll Count	The number of network polls that timed out
Currently Active Poll Count	The number of currently active polls (long-held connections to the server)
Currently Active Session Count	Current number of endpoints registered in the Mobility Service
Currently Active Session Count with Active Presence Subscriptions	The number of currently active sessions with active presence subscriptions
Push Notification Requests Failed/Second	The per second rate of failed push notifications
Push Notification Requests Succeeded/Second	The per second rate of successful push notifications
Push Notification Requests Throttled/Second	The per second rate of throttled push notifications

COUNTER	DESCRIPTION
Push Notification Requests/Second	The per second rate of sent push notifications
Requests Failed/Second	The per second rate of failed requests
Requests Received/Second	The per second rate of received requests
Requests Rejected/Second	The per second rate of rejected requests
Requests Succeeded/Second	The per second rate of successful requests
Succeeded Initiate Session Requests/Second	The per second rate of successful Get Location requests. Requests to initiate a session consume the most CPU on the server. Peak supported load is 12/second. Sustainability depends on other loads on the server. Initiate a session typically means a sign-in for a user that has been signed out for an extended period of time.
Total Declined Inbound Voice Calls	The total number of inbound voice calls that were declined
Total Failed Inbound Voice Calls	The total number of inbound voice calls that failed
Total Failed Outbound Voice Calls	The total number of outbound voice calls that failed
Total number of sessions terminated by user	The total number of sessions terminated by users
Total Push Notification Requests	The total number of push notification requests
Total Push Notification Requests Failed	The total number of push notification requests that failed
Total Push Notification Requests Succeeded	The total number of push notification requests that were successful
Total Push Notification Requests Throttled	The total number of push notification requests that were throttled
Total Requests Failed	The total number of requests that failed
Total Requests received on the Command Channel	The total number of requests received on the command channel
Total Requests Rejected	The total number of requests that were rejected
Total Requests Succeeded	The total number of requests made to the Mobility Service that succeeded
Total Session Initiated Count	The total number of sessions that were initiated since the Mobility Service was started
Total Sessions Terminated Because of User Idle Timeout	The total number of sessions that were terminated because of user idle timeout
Total Successful Inbound Voice Calls	The total number of inbound voice calls that were successful



<b>COUNTER</b>	<b>DESCRIPTION</b>
Total Successful Outbound Voice Calls	The total number of outbound voice calls that were successful

**NOTE**

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

# UCWA events in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Unified Communications Web API (UCWA) in Skype for Business Server.

Skype for Business Server uses the Unified Communications Web API (UCWA) for a number of purposes, from accessing Microsoft Exchange for contact searches to updating presence for mobile clients.

UCWA will write records of operational behavior as event types Informational, Warning, and Error. The following table describes the events that can be written by the UCWA components.

EVENT ID	EVENT TYPE	SUMMARY	CAUSE AND RESOLUTION
20001	Informational	UCWA initialized	N/A N/A
20002	Error	UCWA encountered an unexpected exception during initialization	An unexpected error has occurred during initialization Examine the exception details in the associated event log entry to determine the possible cause
20003	Error	UCWA encountered an unhandled exception	An unhandled exception happened Restart the server. If the problem persists contact product support
20004	Error	Cannot access Exchange for HD photo	Connection to Exchange is not available Make sure the connection to Exchange is available
20005	Informational	Recovered from failing to access Exchange for HD photo	N/A
20006	Error	Cannot access Exchange for contact search	Connection to Exchange is not available Make sure the connection to Exchange is available
20007	Informational	Recovered from failing to search contact in Exchange	N/A
20008	Warning	Attempt to subscribe more than the allowed presence subscriptions per application	Attempt to subscribe more than the allowed presence subscriptions per application Check the clients for unnecessary subscriptions

EVENT ID	EVENT TYPE	SUMMARY	CAUSE AND RESOLUTION
20009	Warning	Attempt to subscribe more than the allowed presence subscriptions per batch	Attempt to subscribe more than the allowed presence subscriptions per batch Check the clients for unnecessary subscriptions
20010	Error	Cannot retrieve inband data	Cannot retrieve inband data If the problem persists contact product support
20011	Error	Cannot subscribe presence	Cannot subscribe presence If the problem persists contact product support
20012	Error	Failed to register endpoint	Failed to register endpoint If the problem persists contact product support
20013	Error	IM MCU is unavailable	IM MCU is unavailable See whether IM MCU is running
20014	Informational	Recovered from failing to connect to IM MCU	N/A
20015	Error	AV MCU is unavailable	AV MCU is unavailable See whether AV MCU is running
20016	Informational	Recovered from failing to connect to AV MCU	N/A
20017	Error	AS MCU is unavailable	AS MCU is unavailable See whether AS MCU is running
20018	Informational	Recovered from failing to connect to AS MCU	N/A
20019	Error	Data MCU is unavailable	Data MCU is unavailable See whether Data MCU is running
20020	Informational	Recovered from failing to connect to Data MCU	N/A
20021	Error	Cannot join IM MCU	Cannot join IM MCU See whether IM MCU is running
20022	Error	Cannot join AV MCU	Cannot join AV MCU See whether AV MCU is running

<b>EVENT ID</b>	<b>EVENT TYPE</b>	<b>SUMMARY</b>	<b>CAUSE AND RESOLUTION</b>
20023	Error	Cannot join AS MCU	Cannot join AS MCU See whether AS MCU is running
20024	Error	Cannot join Data MCU	Cannot join Data MCU See whether Data MCU is running
20025	Error	Cannot access active directory for photo	Connection to active directory is not available Make sure the connection to active directory is available
20026	Informational	Recovered from failing to access active directory for photo	N/A
20027	Warning	Cannot deserialize	Cannot deserialize If the problem persists contact product support

# Using Monitoring Reports in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about Monitoring Reports in Skype for Business Server.

Skype for Business Server includes a set of standard reports that are published by Microsoft SQL Server Reporting Service. These reports, which are accessible by using a web browser, provide usage, call diagnostic information, and media quality information, all based on call detail recording (CDR) and Quality of Experience (QoE) records stored in the CDR and QoE databases.

To use these reports, you must install Monitoring Reports on a computer that is running an instance of the SQL Server.

## In This Section

- [Using the Monitoring Dashboard in Skype for Business Server](#) Provides administrators with a quick overview of their system health and system usage.
- [System usage reports in Skype for Business Server](#) Provides system usage information based on CDR data collected by Skype for Business Server.
- [Call Diagnostic Reports \(per user\) in Skype for Business Server](#) Provides per-user information about failed peer-to-peer and conferencing sessions.
- [Call Diagnostic Reports in Skype for Business Server](#) Provides summary information and diagnostic data for failed peer-to-peer and conferencing sessions.
- [Media Quality Diagnostic Reports in Skype for Business Server](#) Provides information about call quality as well as diagnostic and troubleshooting information for failed calls.

## Locating Records

Monitoring Reports only show a limited number of records on the screen at any one time. The actual number of records displayed on a screen varies depending on the report. To view the records that are not currently shown on the screen you can use the standard forward and backward control (found on each report's toolbar) that enable you to page through the data. You can also quickly jump to the first page or the last page of the dataset.

In addition to using the forward and backward controls, you can also jump to any page in the dataset simply by typing the page number in the **Current Page** box, and then press ENTER.

In addition to providing the ability to page through the data, each report also includes the limited ability to find records. To find records based on a given value, type that value into the **Find** box, and then click **Find**. The report begins searching through the data and stops on the first instance of the value that you entered in the **Find** box. To find the next record that meets the search criteria, click **Next**.

As noted, the Monitoring Reports provide only the most basic search functions. For example, you cannot specify which field the value should be found in. The search mechanism automatically searches for matching values in every field in every record. You cannot use wildcards in your searches, and all searches look for partial values. That means that if you search for 111 the search returns the value 111 along with the values 11100, 811, 3112, 611A5B, and any other fields that include the value 111 anywhere within that field.

Each report is configured to show a default set of records. For example, by default the User Registration Report shows user registration activities for the past week. In some cases, this might result in a report that returns no records. In this case, it means that no user registrations have taken place in the past week. If you see the message "No results match the report filters," try changing the filter values (for example, change the time period to the past month rather than the past week) and rerun the query. For details, see the "Filtering Data" section later in this topic.

## Filtering Data

There will likely be times when you want to look at only a subset of records. For example, only peer-to-peer sessions as opposed to both peer-to-peer sessions and conference sessions. Likewise, there will be times when you need to reduce the number of records that are returned. By default, a report can only display the first 1,000 records in a data set. To address these issues, most reports include a number of filtering options. For example, if you want to view only records for the time period January 1, 2011 through January 15, 2011, you can enter January 1, 2011 in the **From** box and January 15, 2011 in the **To** box. If you then click **View Report**, the returned data will be limited to activities that took place between January 1, 2011 and January 15, 2011.

The filters available to you vary depending on the report that you are viewing. For details about a specific report, see the help topic for that report.

## Exporting Data

The Monitoring Reports provide at least two different ways to export the data included in a report. You can use the **Export** option in the toolbar that appears at the top of each report. To use this option, select the desired export format from the **Select a format** drop-down list. The following formats are available to you:

- XML file with report data
- CSV (comma delimited)
- Acrobat (PDF) file
- MHTML (web archive)
- Excel
- TIFF file
- Word

After selecting a format, click **Export**. When the **File Download** dialog box appears, click **Save**. In the **Save As** dialog box, select a destination folder, enter a file name, and then click **Save**.

If you have Microsoft OneNote installed, you can also copy the report data to OneNote. To do this, right-click the **View Report** button on the toolbar. In the **Select Location in OneNote** dialog box select the section in OneNote where you want to copy the data, and then click **OK**.

# Using the Monitoring Dashboard in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Monitoring Dashboard in Skype for Business Server.

The Monitoring Dashboard provides administrators with a quick overview of their Skype for Business Server system health and system usage. The Dashboard is designed to show an aggregate view of key system metrics and to do so by displaying either:

- Totals for the current day. Note that values shown for the current day represent data that has been recorded from midnight until the current time (based on the local time of the reporting server). That means that you will typically be viewing data for a partial day and not for a 24-hour period. For example, if the local time of the server is 8:00 AM, you see eight hours' worth of data because there are eight hours between midnight and the current time of 8:00 AM.
- Totals for the week, and trend totals for the past six weeks.
- Totals for the month, and trend totals for the past six months (for system usage only).

Note that you can use the [Get-CsReportingConfiguration](#) cmdlet to return the URL used for accessing Skype for Business Server Monitoring Reports:

```
Get-CsReportingConfiguration
```

By default, the Monitoring Dashboard shows data for the following metrics for the current week (and trend totals for the previous six weeks):

## System Usage Metrics

### Registration

- Unique user logons

#### Peer-to-peer

- Total sessions
- IM sessions
- Audio sessions
- Video sessions
- Application sharing
- Total audio session minutes
- Avg. audio session minutes

#### Conference

- Total conferences
- IM conferences

- A/V conferences
- Application sharing conferences
- Web conferences
- Total organizers
- Total A/V conference minutes
- Avg. A/V conference minutes
- Total PSTN conferences
- Total PSTN participants
- Total PSTN participant minutes

In addition to the System Usage metrics, the following metrics displays total for the current day and the previous six days (if you select **Weekly View**) or for the current week and the past six weeks if you select **Monthly View**.

## Per-User Call Diagnostics

### Users with call failures

- Total users with call failures
- Conference organizers with call failures

### Users with poor quality calls

- Total users with poor quality calls

## Call Diagnostics

### Peer-to-peer

- Total failures
- Overall failure rate
- IM failure rate
- Audio failure rate
- Application sharing failure rate

### Conference

- Total failures
- Overall failure rate
- IM failure rate
- A/V failure rate
- Application sharing failure rate

### Top five servers by failed sessions

## Media Quality Diagnostics



Peer-to-peer

- Total poor quality calls
- Poor quality call percentage
- PSTN calls with poor quality

Conference

- Total poor quality calls
- Poor quality call percentage
- PSTN calls with poor quality

Top worst servers by poor quality call percentage

## Working with the Monitoring Dashboard

As noted, by default totals are shown for the current week and trend values are shown for the past six weeks. If you would prefer to see totals for the current month (as well as trend values for the past six months), click the **Monthly View** link in the upper right corner of the dashboard. If you decide to view monthly totals, the link text will change to **Weekly View**. You can switch back to the weekly view by clicking that link.

### TIP

The Monitoring Dashboard restricts you to looking at totals for the current week (or month) and trend values for the past six weeks (or months). You cannot change these dates and times. For example, you cannot use the Dashboard to view report totals for the time period beginning nine months ago.

The values shown in the **This week**, **This month**, or **Today** columns link you to more detailed information about the item. Keep in mind that the column name and the values displayed in that column will often differ depending on the metric chosen and depending on whether you have selected weekly view or monthly view. For example, if you click the totals shown for the **Unique user logons** metric you will see the **User Registration Report** for the specified time period. You can return to the Monitoring Dashboard at any time by clicking **Dashboard**.

### TIP

You can also access the Monitoring Server Reports home page by clicking the **Reports** link in the upper right corner of the Dashboard.

The **Trend** column displays a simple line graph that shows totals for the past six weeks (or, depending on the metric and the time interval, the past six days or the past six months). These simple line graphs display one unlabeled data point for each time period (for example, one unlabeled data point for each of the past six weeks). However, you can retrieve actual values for these graphs by holding your mouse pointer over the graph. In that case, a tool tip shows you the maximum and minimum values in the graph.

## Exporting Data from the Monitoring Dashboard

The Monitoring Dashboard provides a number of ways to export the current dashboard view. On the Dashboard toolbar, you'll see an icon that looks like a floppy disk with a green arrow attached to it. If you click this icon, a dropdown list will appear giving you the following data export formats:

- XML file with report data

- CSV (comma delimited)
- PDF
- MHTML (web archive)
- Excel
- TIFF file
- Word

To export the current dashboard view (and its values), click the desired export option. Skype for Business Server generates a report in the specified format and then give you the option of opening that report or saving it. Note that, by default, Skype for Business Server titles the report **Monitoring Dashboard** and saves it to your Downloads folder. To give the report a different name or to store it in a different folder, click the arrow next to the **Save** button and then click **Save As**. If you are fine with name **Monitoring Dashboard** and with having the report saved in the Downloads folder you can just click the **Save** button.

It's possible that, when you try to export dashboard data, a **Security Alert** dialog box will appear along with the message "Your current settings do not allow this file to be downloaded." If that occurs, do the following:

- In Internet Explorer, select **Internet Options**.
- In the **Internet Options** dialog box, on the **Security** tab, click **Trusted sites** and then click **Sites**.
- In the **Trusted sites** dialog box, click **Add** to add the Skype for Business Server that is running Skype for Business Server Reports to the collections of trusted websites.
- Click **Close** and then click **OK**.

You will then need to refresh the Monitoring Dashboard before the changes take effect. To do that, either press F5 or click the **Refresh** icon in the Dashboard toolbar. (The **Refresh** icon is a circle with a pair of green arrows in it.)

You can also create an Excel spreadsheet that includes live data feeds, which includes links to the latest Monitoring Dashboard data. To create a live data feed file, click the orange **Export to Data Feed** icon in the toolbar.

If you would prefer to print the current Dashboard then click the printer icon in the toolbar.

# System usage reports in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the System Usage Reports in Skype for Business Server.

The System Usage Reports provide system usage information based on call detail recording (CDR) data collected by the Skype for Business Server.

## In this section

- [User Registration Report in Skype for Business Server](#)

Provides a summary of user connectivity to the Skype for Business Server deployment based on registration events such as user logons. The report provides a way to view both internal and external logons, and to compare the number of users who logged on to Skype for Business Server with the number of users who actually used the service while they were logged on.

- [Peer-to-Peer Activity Summary Report in Skype for Business Server](#)

Provides a summary of peer-to-peer instant messaging (IM), audio, video, file transfer, and application sharing sessions. Peer-to-peer sessions are sessions involving just two users.

- [Conference Summary Report in Skype for Business Server](#)

Provides a summary of all conference activities. Conferences are sessions involving three or more people.

- [PSTN Conference Summary Report in Skype for Business Server](#)

Provides a summary of all PSTN conferences. These are conferences where at least one user dials in using the public switched telephone network (PSTN), which is also referred to as dial-in conferencing.

- [Response Group Usage Report in Skype for Business Server](#)

Provides a summary of Response Group usage. The Response Group application provides a way for you to automatically route phone calls to entities such as a help desk or customer support line.

- [IP Phone Inventory Report in Skype for Business Server](#)

Provides information about the IP phones currently in use in the organization. The report is based on phone registrations and logons. It should not be considered a complete inventory. For example, you might have removed phones that are still listed in the report because they logged on at least once. Likewise, you might also have new phones that do not show up in the report simply because users have not logged on to Skype for Business Server with their new phones yet.

- [Call Admission Control Report in Skype for Business Server](#)

Provides a list of peer-to-peer and conference activities that use call admission control. Call admission control (CAC) is a way of determining whether you should allow real-time communications sessions, such as voice or video calls, based on bandwidth constraints.

# User Registration Report in Skype for Business Server

5/20/2019 • 8 minutes to read

**Summary:** Learn about the User Registration Report in Skype for Business Server.

The User Registration Report provides an overview of user logon activity, most notably information about the number of users who logged on to Skype for Business Server during a specified time period (hourly, daily, weekly, monthly). Keep in mind that the report only tells you how many people logged on. It does not tell you which people logged on. Monitoring Reports do not provide information about which specific users are using Skype for Business Server (and which ones are not). However, you can get a rough estimate of user information by using the User Activity Report.

When providing information about user logons, the User Registration Report draws two important distinctions. First, it breaks logons down into two primary categories: internal logons and external logons. Internal logons represent users who logged on from inside your organization's firewall (that is, while connected to the corporate network). External logons represent users who logged on from outside the firewall through an Edge Server (for example, a user who logged on from an Internet café counts as an external logon). If you need to know how many of your users are logging on from outside the firewall, the User Registration Report can provide you with this information.

In addition, the User Registration Report notes how many active users were present during a given time period. An active user is a user who took part in an instant messaging (IM) session, participated in a Skype for Business Server Meeting, made or received a phone call, or otherwise used Skype for Business Server during that period of time. This is different from a user who logged on, but never actually used the system.

## Accessing the User Registration Report

You access the User Registration Report only from the Monitoring Reports home page. The User Registration Report does not link to any other reports.

## Making the Best Use of the User Registration Report

After you've deployed Skype for Business Server one commonly-asked question is this: How do I know if my users are actually using this new technology? Although it has a few limitations in this regard, the User Registration Report can help you answer this question. To determine whether or not users are using Skype for Business Server, you need to do two things. First, get the value of the Unique logon users metric from the User Registration Report. This value tells you how many distinct individuals logged on to Skype for Business Server.

By comparison, the Total logons metric shows how many total times anyone logged on to Skype for Business Server. For example, suppose Ken Myer logged on to Skype for Business Server five different times in a single day. In that case, Ken Myer would count as five separate logon sessions for the Total logons metric, but just one logon user for the Unique logon users metric. Likewise, it's not uncommon for a user to log on from multiple devices or multiple locations. For example, a user can log on using her desktop computer, her laptop computer, and she can have an IP phone that automatically logs on to Skype for Business Server. In this example, there is one unique user with three logons.

To further explain the difference between total logons and unique logons, consider the logons for a given time period in the following table.

USER	LOGON TIME
Ken Myer	7/7/2015 8:45 AM
Ken Myer	7/7/2015 8:46 AM
Pilar Ackerman	7/7/2015 9:17 AM
Ken Myer	7/7/2015 9:22 AM
Pilar Ackerman	7/7/2015 9:31 AM

Notice that there is a total of five logons; however, there are only two unique logon users: Ken Myer (who logged on three times) and Pilar Ackerman (who logged on twice). That's the difference between logons and unique logon users.

In addition to knowing the number of unique logons, you need to know the total number of users who have been enabled for Skype for Business Server. That value can be retrieved by opening the Skype for Business Server Management Shell and running the following Windows PowerShell command:

```
(Get-CsUser).Count
```

If the preceding command returns a value of 1,236 and Unique logon users metric returns an average value of 667, that suggests that a little over half of your users enable for Skype for Business are actually logging on to the system each day (that is, 667 divided by 1,236, which is approximately 54%).

#### Caution

Keep in mind that the logon metrics record users who actually logged on during the specified time period. They don't keep track of users who were already logged on to the system. For example, if your Unique logon users metric shows 667 logons and you have 1,236 users, that suggests that about half your users are logging on to the system. However, suppose 300 users were already logged on to the system at the time you began checking the logon data. That would mean that you actually had nearly 1,000 users logged on to Skype for Business Server, which would mean that closer to 80% of your users were logged on.

You should also compare the Unique logon users value with the value of the Unique active users metric. The Unique active users metric tells you how many unique users actually used Skype for Business Server: they made a phone call, they joined a Skype for Business Server Meeting, or they participated in an IM session. This is useful information, because Skype for Business Server can be configured to automatically start each time a user starts Windows. Because of that, you might have a large number of users who automatically log on to Skype for Business when they log on to Windows each day, but then never actually use Skype for Business Server during that time period.

The Unique active users metric also provides more meaningful data in an organization where users typically do not log off Windows at the end of the day. Instead, they simply lock their computers and leave Windows and Skype for Business running. In a situation like that, you might end up with very few logons per day because your users logged on several days ago and never logged off. However, Unique active users tells you whether users are actively using Skype for Business or another Skype for Business Server client.

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. For example, the User Registration Report enables you to view data for all your Registrar pool and Edge Servers or to view data for an individual pool. You can also choose how data should be grouped. In this case, registrations grouped by hour, day, week, or month.

The following table lists the filters that you can use with the User Registration Report.

### User Registration Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) are displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Pool</b>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or choose <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>

## Metrics

The following table lists the information provided in the User Registration Report.

### User Registration Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Hourly</b> <b>Daily</b> <b>Weekly</b> <b>Monthly</b>	No	<p>Indicates the time interval that you selected on the filter toolbar. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2015, you see an hourly breakdown of user registration activity for that date.</p>
<b>Total logons</b>	No	Total number of successful logon sessions.
<b>Internal logons</b>	No	Total number of logons within the internal network.
<b>External logons</b>	No	Total number of logons from outside the internal network, using the Edge Server.
<b>Unique logon users</b>	No	Total number of users who had at least one logon session. A user who had multiple logon sessions counts as one user, the same as a person who had just a single logon session.
<b>Unique active users</b>	No	Total number of users who were involved in a peer-to-peer or conferencing session. A user who had multiple sessions counts as one user, the same as a person who had just a single session.

# Peer-to-Peer Activity Summary Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Peer-to-Peer Activity Summary Report in Skype for Business Server.

The Peer-to-Peer Activity Summary Report provides an overall view of your peer-to-peer communication sessions. A peer-to-peer session typically involves just two users, and does not require the use of the Skype for Business Server conferencing services. By comparison, a conference typically involves more than two users and requires the use of Skype for Business Server conferencing services. Conference activity is reported on the Conference Summary Report.

The Peer-to-Peer Activity Summary Report helps you answer questions like the following:

- How many peer-to-peer instant messages do my users send on a typical day?
- Are any of my users actually taking advantage of the Skype for Business Server application sharing and file transfer capabilities?
- Users have been complaining that the network seems slow at certain times of the day. How many minutes are devoted to peer-to-peer audio and video sessions during those time periods?

## Accessing the Peer-to-Peer Activity Summary Report

You access the Peer-to-Peer Activity Summary Report from the Monitoring Reports home page. You open the [Peer-to-Peer IM Report in Skype for Business Server](#) by clicking either of the following metrics:

- Total peer-to-peer IM sessions
- Total peer-to-peer IM messages

Likewise, you can open the Peer-to-Peer Voice and Video Report by clicking any of these metrics:

- Total peer-to-peer audio sessions
- Total peer-to-peer audio session minutes
- Total peer-to-peer video sessions
- Total peer-to-peer video session minutes

## Making the Best Use of the Peer-to-Peer Activity Summary Report

At the bottom of the Peer-to-Peer Activity Summary Report you'll find totals for metrics such as Total peer-to-peer IM sessions and Total peer-to-peer IM messages. This provides a quick summary of the detailed information found in the body of the report.

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. For example, the Peer-to-Peer Activity Summary Report enables you to choose how data should be grouped. In this case, activity grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Peer-to-Peer Activity Summary Report.



## Peer-to-Peer Activity Summary Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/17/12015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/17/12015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/17/12015 and an end date of 2/28/2015, data is displayed for the days 8/7/12015 12:00 AM to 9/7/12015 12:00 AM (that is, a total of 31 days' worth of data).</p>

## Metrics

The following table lists the information provided in the Peer-to-Peer Activity Summary Report.

### Peer-to-Peer Activity Summary Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Hourly</b> <b>Daily</b> <b>Weekly</b> <b>Monthly</b>	No	Indicates the time interval that you selected on the filter toolbar. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/17/12015, you see an hourly breakdown of user registration activity for that date.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Total peer-to-peer sessions</b>	No	Total number of peer-to-peer sessions conducted, regardless of session type.
<b>Total peer-to-peer IM sessions</b>	No	Total number of peer-to-peer instant messaging (IM) sessions. When you click this item, the report shows you the Peer-to-Peer IM Report for the selected time period.
<b>Total peer-to-peer IM messages</b>	No	Total number of instant messages sent in peer-to-peer sessions. When you click this item, the report shows you the Peer-to-Peer IM Report for the selected time period.
<b>Total peer-to-peer audio sessions</b>	No	Total number of peer-to-peer audio calls. When you click this field, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
<b>Total peer-to-peer audio session minutes</b>	No	Total amount of time spent in peer-to-peer audio sessions. When you click this item, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
<b>Average peer-to-peer audio session minutes</b>	No	Average amount of time spent in peer-to-peer audio sessions. Calculated by dividing the total audio session time by the total number of audio sessions.
<b>Total peer-to-peer video sessions</b>	No	Total number of peer-to-peer video calls. Note that video sessions are also counted as audio sessions: each video session is counted as one video session and one audio session. When you click this item, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
<b>Total peer-to-peer video session minutes</b>	No	Total amount of time spent in peer-to-peer video sessions. When you click this item, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
<b>Average peer-to-peer video session minutes</b>	No	Average amount of time spent in peer-to-peer video sessions. Calculated by dividing the total video session time by the total number of video sessions.
<b>Total peer-to-peer file transfer sessions</b>	No	Total number of peer-to-peer sessions that included file transfers.
<b>Total peer-to-peer application sharing sessions</b>	No	Total number of peer-to-peer sessions that included application sharing.



# Peer-to-Peer IM Report in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn about the Peer-to-Peer IM Report in Skype for Business Server.

The Peer-to-Peer IM Report provides trend information about peer-to-peer instant messaging (IM) sessions, broken down by pool and by authentication type. The report can show either the total number of sessions held during the specified time period (for example, day-by-day or hour-by-hour), or it can show the total number of instant messages sent during that time period.

## Accessing the Peer-to-Peer IM Report

You can access the Peer-to-Peer IM Report only by opening the [Peer-to-Peer Activity Summary Report in Skype for Business Server](#) and then clicking either of the following metrics:

- Total peer-to-peer IM sessions
- Total peer-to-peer IM messages

## Making the Best Use of the Peer-to-Peer IM Report

By default, the Peer-to-Peer IM Report shows you the message count per-hour (or day, depending on your settings). However, you can also choose to view the day by sessions per hour. To do that, click **Hide/Show Parameters** in the upper-right corner of the Reports window, and then click **Session Count** from the **Report by** list.

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Peer-to-Peer IM Report.

### Peer-to-Peer IM Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>To</b>	<p>End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval then only the maximum number of values (starting from the start date) are displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Report by</b>	<p>Indicates the values to be used in the report. Select one of the following: Session count Message count</p>

## Metrics for Peer-to-Peer IM Session by Pool

The following table lists the information provided in the Peer-to-Peer IM Report.

### Metrics for Peer-to-Peer IM Session by Pool

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Pool</b>	No	Name of the Registrar pool or Edge Server.
<b>Date/Time</b>	No	Date and time that the sessions took place.
<b>Total</b>	No	Total number of sessions or total message count.

## Metrics for Peer-to-Peer IM Session by Authentication Type

The following table lists the information provided in the Peer-to-Peer IM Report for each type of authentication used by the participants in a peer-to-peer session.

### Metrics for Peer-to-Peer IM Session by Authentication Type

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Authentication type</b>	No	Type of authentication used by the session participants. Values are typically one of the following: Enterprise Federated PIC
<b>Date/Time</b>	No	Date and time that the sessions took place.
<b>Total</b>	No	Total number of sessions or total message count.

# Peer-to-Peer Voice and Video Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Peer-to-Peer Voice and Video Report in Skype for Business Server.

The Peer-to-Peer Voice and Video Report provides a detailed look at the distribution of voice and video calls over a specified period of time (for example, calls per hour or calls per day). The report also gives you the option of viewing all the voice and video calls that were made, or of viewing only the successful or failed calls. The reports shows call information broken down into the following groupings:

- Calls per pool
- Calls per call type (for example, a Skype for Business to Skype for Business call vs. a Skype for Business call to a person on the PSTN network)
- Calls per access type (users logged on to the internal network vs. users logged on to the external network)
- Calls per Mediation Server

## To access the peer-to-peer voice and video report

You can access the Peer-to-Peer Voice and Video Report only by opening the Peer-to-Peer Activity Summary Report and then clicking any of the following metrics:

- Total peer-to-peer audio sessions
- Total peer-to-peer audio minutes
- Total peer-to-peer video sessions
- Total peer-to-peer video minutes

## To make the best use of the peer-to-peer voice and video report

There are a number of ways you can filter the Peer-to-Peer Voice and Video Report. However, those filtering options are hidden from view by default. To view the filtering options available to you, click **Show/Hide Parameters** button in the upper-right corner of the Report window.

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the data in different ways. The following table lists the filters that you can use with the Peer-to-Peer Voice and Video Report.

### Peer-to-peer voice and video report filters

NAME	DESCRIPTION
------	-------------

NAME	DESCRIPTION
<b>From</b>	<p>Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Media type</b>	<p>Indicates the type of media used in the session. Select one of the following: Both Audio Video</p>
<b>Call disposition</b>	<p>Indicates the success or failure of the session. Select one of the following: [All] Success Calls Failed Calls</p>
<b>Report by</b>	<p>Indicates the values to be used in the report. Select one of the following: Session count Call minutes</p>

## Metrics for peer-to-peer voice and video activity by Pool



The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each pool.

### Metrics for peer-to-peer voice and video activity by pool

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Pool</b>	No	Name of the Registrar pool or Edge Server used for the call.
<b>Date/Time</b>	No	Date and time period in which the call took place.
<b>Total</b>	No	Total number of sessions or total message count.

### Metrics for peer-to-peer voice and video activity by call type

The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each type of call that was made.

### Metrics for peer-to-peer voice and video activity by call type

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call type</b>	No	Indicates the type of call that was made. Values are one of the following: UC-to-UC UC-to-PSTN PSTN-to-UC PSTN-to-PSTN
<b>Date/Time</b>	No	Date and time period in which the call took place.
<b>Total</b>	No	Total number of sessions or total message count.

### Metrics for peer-to-peer voice and video activity by access type

The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each network access type.

### Metrics for peer-to-peer voice and video activity by access type

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Activity type</b>	No	Indicates whether the clients were logged on to the internal network or the external network when the call was placed. Values are typically one of the following: Internal External Mixed
<b>Date/Time</b>	No	Date and time period in which the call took place.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
------	----------------------------	-------------

<b>Total</b>	No	Total number of sessions or total message count.
--------------	----	--

## Metrics for peer-to-peer voice and video activity by mediation server

The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each Mediation Server.

### Metrics for peer-to-peer voice and video activity by mediation server

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Mediation Server</b>	No	Name of the Mediation Server.
<b>Date/Time</b>	No	Date and time period in which the call took place.
<b>Total</b>	No	Total number of sessions or total message count.

# Conference Summary Report in Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Learn about the Conference Summary Report in Skype for Business Server.

The Conference Summary Report provides an overall view of your online conferencing sessions. A conference typically involves more than 2 users and requires the use of conferencing services. By comparison, a peer-to-peer session typically involves just 2 users and does not require the use of Skype for Business Server conferencing services. Peer-to-peer activities are reported on the [Peer-to-Peer Activity Summary Report in Skype for Business Server](#).

The Conference Summary Report not only tells you how many conferences were held during a given time period (hourly, daily, weekly, monthly) but also tells you the total number of people who took part in those conferences, and the total number of unique conference organizers.

A "unique" organizer is anyone who schedules at least one conference. For example, if Pilar Ackerman schedules one conference she counts as one unique organizer. If Ken Myer schedules 148 conferences he, too counts as one unique organizer. For example, the following table shows 8 conferences scheduled, but just three unique organizers (Ken Myer, Pilar Ackerman, and David Ahs).

CONFERENCE ORGANIZER	CONFERENCE DATE
Ken Myer	7/7/2015 10:00 AM
David Ahs	7/7/2015 10:00 AM
Ken Myer	7/7/2015 11:00 AM
Pilar Ackerman	7/7/2015 11:00 AM
Ken Myer	7/7/2015 1:00 PM
Pilar Ackerman	7/7/2015 2:00 PM
Ken Myer	7/2/2015 10:00 AM
Pilar Ackerman	7/2/2015 10:00 AM

The Conference Summary Report also indicates how many conferences included audio and/or video.

## Accessing the Conference Summary Report

The Conference Summary Report is accessed from the Monitoring Reports home page. You can drill down to the Conference Activity report by clicking either of the following metrics:

- Total conferences
- Total participants

# Making the Best Use of the Conference Summary Report

Total values for most of the metrics used on the Conference Summary Report can be found at the bottom of the report; scroll down to see values such as the total number of conferences held during the specified time period, and the total number of people who participated in those conferences. One metric that is not totaled at the bottom of the report is Total unique conference organizers. Why not? Here's one reason. Suppose you are looking at a month's worth of data. On day 1 you had 34 unique conference organizers; on day 2 you had 27 unique conference organizers. Does that mean you had 61 unique conference organizers for those two days? Not necessarily. After all, all 27 people who organized conferences on day 2 might be among the 34 people who organized conferences on day 1. For example, in this simple report, note that Ken Myer and Pilar Ackerman scheduled conferences both on 7/7/2015 and on 7/2/2015:

CONFERENCE ORGANIZER	CONFERENCE DATE
Ken Myer	7/7/2015 10:00 AM
David Ahs	7/7/2015 10:00 AM
Ken Myer	7/7/2015 11:00 AM
Pilar Ackerman	7/7/2015 11:00 AM
Ken Myer	7/7/2015 1:00 PM
Pilar Ackerman	7/7/2015 2:00 PM
Ken Myer	7/2/2015 10:00 AM
Pilar Ackerman	7/2/2015 10:00 AM

To get a better idea of the total number of unique users who organized conferences, change your time interval; for example, look at the data by month instead of by day.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Conference Summary Report enables you to choose how data should be grouped. In this case, conferences grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Conference Summary Report.

### Conference Summary Report Filters

NAME	DESCRIPTION
------	-------------

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) are displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>

## Metrics

The following table the information provided by the Conferences Summary Report.

### Conference Summary Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Hourly</b> <b>Daily</b> <b>Weekly</b> <b>Monthly</b>	No	Indicates the time interval that you selected on the filter toolbar. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2015, you see an hourly breakdown of user registration activity for that date.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Total conferences</b>	No	Total number of conferences (regardless of conference type) that were held. When you click this item, the report shows you the Conference Activity Report for the selected time period.
<b>Total participants</b>	No	Total number of people who took part in the conferences. When you click this item, the report shows you the Conference Activity Report for the selected time period.
<b>Average participants per conference</b>	No	Average number of people who took part in a given conference. Determined by dividing the total conferences by the total participants.
<b>Total A/V conferences</b>	No	Total number of conferences that included audio or video.
<b>Total A/V conference minutes</b>	No	Total number of minutes devoted to audio/video conferencing. The Total A/V conference minutes metric summarizes all the audio/visual conference types, including: A/V conferences; IM conferences; app sharing conferences; data conferences; and PSTN conferences.
<b>Total A/V conference participant minutes</b>	No	Total number of participant minutes devoted to audio/video conferencing. For example, suppose one user spends 5 minutes in an audio/video conference and a second user spends 3 minutes in that same conference. That makes a total of 8 participant minutes: 5 minutes plus 3 minutes.
<b>Average A/V conference minutes</b>	No	Average number of minutes per audio/video conference.
<b>Total number of unique organizers of conferences</b>	No	Total number of users who organized at least one conference. Users who organized more than one conference are counted as one unique organizer, just like users who only organized a single conference.
<b>Total conference messages</b>	No	Total number of instant messages sent during the conferences.

# Conference Activity Report in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Conference Activity Report used in Skype for Business Server.

The Conference Activity Report makes it easy for you to answer questions like these: how many conferences are being held each day, and when are those conferences being held? Information like this is useful not only in its own right, but also as a troubleshooting tool. For example, suppose users are complaining that the network seems particularly slow in the middle of the day. A quick glance at the Conference Activity reports might suggest one possible reason: far more conferences are being scheduled between the hours of 10:00 AM and 2:00 PM than at any other time.

If the slow network is causing problems, you can encourage users to reschedule some of their conferences during the less-heavily trafficked times of the day.

## Accessing the Conference Activity Report

The Conference Activity Report is accessed from the [Conference Summary Report in Skype for Business Server](#) by clicking either one of the following metrics:

- Total conferences
- Total participants

## Making the Best Use of the Conference Activity Report

By default the Conference Activity Report shows you the total number of conferences for the specified time period (for example, the total number of conferences per day, or the total number of conferences per hour of the day).

However, you can also choose to display the total number of participants for that time period or the total number of participant minutes. To do that, click the Show/Hide Parameters button to display the filtering options, and then select one of the following from the Report by dropdown list:

- Participant count
- Participant minutes
- Conference count

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Conference Activity Report.

### Conference Activity Report Filters

NAME	DESCRIPTION
------	-------------

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select any of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Report by</b>	<p>Indicates the values to be used in the report. You can select one of the following: Participant Count Participant Minutes Conference Count</p>

## Metrics for Conferences by Pool

The following table lists the information in the Conference Activity Report for each pool.

### Metrics for Conferences by Pool

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Pool</b>	No	Name of the Registrar pool or Edge Server used in the conference.



NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Date/Time</b>	No	Date and time when the conference was held.
<b>Total</b>	No	Total participant count, total participant minutes, or total conference count.

## Metrics for Conferences by Server Type

The following table lists the information in the Conference Activity Report for each type of server.

### Metrics for Conferences by Server Type

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Conferencing server type</b>	No	Type of server used in the conference, typically one of the following: Web Conferencing Server IM Conferencing Server Telephony Conferencing Server AV Conferencing Server Application Sharing
<b>Date/Time</b>	No	Date and time when the conference was held.
<b>Total</b>	No	Total participant count, total participant minutes, or total conference count.

# Conference Detail Report in Skype for Business Server

8/8/2019 • 2 minutes to read

**Summary:** Learn about the Conference Detail Report used in Skype for Business Server.

The Conference Detail Report provides detailed information about all the users who participated in a conference. For example, you can see such information as the date and time that a user joined the conference, the date and time that the user left the conference, and the user agent of the endpoint that was used to connect that user to the conference. You can also see information the user's role in each conference (for example, Presenter or Attendee). Perhaps most important, you get quickly see which users successfully join and complete the conference, and which users were not able to successfully join and complete the conference.

## Accessing the Conference Detail Report

The Conference Detail Report can be accessed from the following reports:

- The [Call Admission Control Report](#) (by clicking the Detail metric for a conference)
- The [Failure List Report](#) (by clicking the Conference metric)
- The [User Activity Report](#) (by clicking the Conference URI metric)

From the Conference Detail Report you can access the [Diagnostic Report](#) by clicking the Diagnostic Report (Detail) metric.

## Filters

None. You cannot filter on the Conference Detail Report.

## Metrics

The following table lists the information provided in the Conference Information section of the Conference Detail Report.

### Conference Information Metrics

NAME	DESCRIPTION
<b>Conference URI</b>	URI assigned to the conference. For example: sip:kmyer@litwareinc.com;gruu;opaque=app:conf:focus:id:dr2y8v4
<b>Pool FQDN</b>	Fully-qualified domain name of the Registrar pool or Edge Server involved in a session.
<b>Start time</b>	Date and time that the conference started.
<b>Organizer</b>	SIP address of the user who organized the conference.
<b>End time</b>	Date and time that the conference ended.

The following table lists the information provided in the Conference Participation Section of the Conference Detail Report.

### Conference Participation Metrics

NAME	DESCRIPTION
<b>User</b>	SIP address of the user who participated in the conference.
<b>Role</b>	Role (for example, Presenter) played by the conference participant.
<b>Connectivity</b>	Network connectivity (typically From Internal or From External) for the participant.
<b>Join time</b>	Date and time that the participant joined the conference.
<b>Leave time</b>	Date and time that the participant left the conference.
<b>User agent</b>	Identifier for the software used by the participant's endpoint.
<b>Diagnostic reports</b>	Provides diagnostic and troubleshooting information. Including SIP response codes, diagnostic headers, conference join times, and diagnostic IDs for failed sessions.

The following table lists the information provided in the Conference Modalities section of the Conference Detail Report.

### Conference Modalities Metrics

NAME	DESCRIPTION
<b>User</b>	SIP address of the user who participated in the conference.
<b>Join time</b>	Date and time that the participant joined the conference.
<b>Leave time</b>	Date and time that a participant left the conference.
<b>Conferencing server URI</b>	URI for the Conferencing server used in the conference.
<b>Diagnostic reports</b>	Provides diagnostic and troubleshooting information. Including SIP response codes, diagnostic headers, conference join times, and diagnostic IDs for failed sessions.

# Conference Join Time Report in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Conference Join Time Summary Report in Skype for Business Server.

The Conference Join Time Summary enables you to determine how long it takes your users to join a conference. The report shows the average join time (in milliseconds), and also provides a breakdown that lets you know how many users were able to join a conference in 2 seconds or less, how many users required between 2 and 5 seconds to join the conference, and so on.

## Accessing the Conference Join Time Report

The Conference Join Time Report is accessed from the Monitoring Reports home page.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Conference Join Time Report.

### Conference Join Time Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>Interval</b>	<p>Time interval. Select one of the following:</p> <ul style="list-style-type: none"> <li>Hourly (a maximum of 25 hours can be displayed)</li> <li>Daily (a maximum of 31 days can be displayed)</li> <li>Weekly (a maximum of 12 weeks can be displayed)</li> <li>Monthly (a maximum of 12 months can be displayed)</li> </ul> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Pool</b>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>
<b>Conference sessions</b>	<p>Type of session. Allowed values are:</p> <ul style="list-style-type: none"> <li>[All]</li> <li>Focus sessions (the Focus is the central policy and state manager for online meetings and coordinates all aspects of A conference)</li> <li>Application sharing</li> <li>A/V conferencing</li> </ul> <p>If you select [All], the total conference join time will be displayed at the top of the report. Note that these totals are only for conferences which were scheduled by using Microsoft Exchange or Microsoft Outlook.</p>

## Metrics

The following table lists the information provided in the Conference Join Time Report.

### Conference Join Time Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<p><b>Date</b></p> <p>The actual title for this metric will vary depending on the Interval that was selected.</p>	No	Date and time that the conference took place.
<b>Total sessions</b>	No	Total number of sessions, including successful sessions, failed sessions (both expected failures and unexpected failures), and uncategorized sessions.
<b>Average (ms)</b>	No	Average amount of time (in milliseconds) that it took participants to join the conference.
<b>Sessions &lt; 2 seconds, Volume</b>	No	Number of participants who were able to join the conference in less than 2 seconds.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Sessions &lt; 2 seconds, Percentage</b>	No	
<b>Sessions 2-5 seconds, Volume</b>	No	Number of participants who took between 2 seconds and 5 seconds to join the conference.
<b>Sessions 2-5 seconds, Percentage</b>	No	Percentage of the total call participants who took between 2 seconds and 5 seconds to join the conference.
<b>Sessions 5-10 seconds, Volume</b>	No	Number of participants who took between 5 seconds and 10 seconds to join the conference.
<b>Sessions 5-10 seconds, Percentage</b>	No	Percentage of the total call participants who took between 5 seconds and 10 seconds to join the conference.
<b>Sessions &gt; 10 seconds, Volume</b>	No	Number of participants who required more than 10 seconds to join the conference.
<b>Sessions &gt; 10 seconds, Percentage</b>	No	Percentage of the total call participants who required more than 10 seconds to join the conference.

# PSTN Conference Summary Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the PSTN Conference Summary Report in Skype for Business Server.

In Skype for Business Server, a PSTN conference is any conference in which at least one participant dials in to the audio portion by using a PSTN (public switched telephone network) phone. (A PSTN phone is a "landline," a cell phone, or any other phone which does not make use of Voice over IP.) Although referred to as PSTN conferences in the Monitoring Reports, these conferences are perhaps more-commonly known as dial-in conferences.

The PSTN Conference Summary Report provides information about all the PSTN conferences held in your organization (that is, all the conferences that had at least one dial-in user). The report includes information about the total number of PSTN conferences, the total number of people who participated in those conferences, and, perhaps, most important, the total number of dial-in users (the Total PSTN participants metric).

## Accessing the PSTN Conference Summary Report

The PSTN Conference Summary Report can only be accessed from the Monitoring Reports home page. This report is not linked to any other reports. Note that you cannot retrieve detailed call information for a PSTN conference, in part because individual endpoints are responsible for submitting this information. PSTN phones are not capable of tracking or submitting call detail information.

## Making the Best Use of the PSTN Conference Summary Report

To determine the percentage of all your conferences that include dial-in users, compare the value of the Total PSTN conferences metric with the Total conferences metric found on the [Conference Summary Report in Skype for Business Server](#).

If you don't see as many PSTN conferences as you might have expected to see, keep in mind that the ability to organize a conference that allows dial-in users depends on the conferencing policy that has been assigned to a user: if very few of your users are allowed to hold PSTN conferences you would obviously see very few PSTN conferences. You can quickly verify which of your conferencing policies (if any) allow users to schedule PSTN conferences by running the following command from within the Skype for Business Server Management Shell:

```
Get-CsConferencingPolicy | Select-Object Identity, EnableDialInConferencing
```

That will return data similar to this:

Identity	EnableDialInConferencing
-----	-----
Global	True
site:Redmond	False
site:Dublin	False
Tag:RedmondDialInUsers	True
Tag:DublinDialInUsers	True

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. For example, the PSTN Conference Summary Report enables you to choose how data should be grouped. In this case, conferences are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the PSTN Conference Summary Report.

### PSTN Conference Summary Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>

## Metrics

The following table lists the information in the PSTN Conference Summary Report.

### PSTN Conference Summary Report Metrics



NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Hourly</b> <b>Daily</b> <b>Weekly</b> <b>Monthly</b>	No	Indicates the selected time interval. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2015, you see an hourly breakdown of user registration activity for that date.
<b>Total PSTN conferences</b>	No	Total number conferences that allowed dial-in access.
<b>Total participants</b>	No	Total number of people who participated in conferences that allowed dial-in access.
<b>Total A/V conference minutes</b>	No	Total amount of audio/visual conference time.
<b>Total A/V conference participant minutes</b>	No	Total amount of audio/visual participant time. For example, if one participant spent five minutes in an A/V conference and another participant spent three minutes in the same conference, the total A/V conference participant time would be eight minutes.
<b>Total PSTN participants</b>	No	Total number of users who dialed in to conferences that allowed dial-in access.
<b>Total PSTN participant minutes</b>	No	Total amount of conference time spent by dial-in users. For example, if one dial-in participant spent five minutes in a conference and another participant spent three minutes in the same conference, the total PSTN participant time would be eight minutes.
<b>Unique conference organizers</b>	No	Total number of users who organized at least one conference that allowed dial-in access. Users who organized more than one conference are counted as one unique organizer, just like users who only organized a single conference.

# Response Group Usage Report in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Learn about the Response Group application in Skype for Business Server.

The Response Group application provides a way for Skype for Business Server to answer and route phone calls based on the number that was dialed and, optionally, on the caller's responses to a series of questions. Typically, Response Group calls are not routed to an individual person but, instead, are routed to a team of people referred to as an agent group. For example, if someone calls the phone number for your help desk, Skype for Business Server can automatically route that call to the first available help desk agent. Alternatively, Skype for Business Server could ask a series of questions ("Press 1 if you are having hardware problems. Press 2 if you are having software problems. Press 3 if you are having network problems."), and then route the call to the most appropriate help desk agent based on the answer to those questions.

The Response Group Usage Report provides a detailed look at the number of phone calls received by all your Response Group workflows, then breaks those calls down into more finite categories such as Offered calls, Answered calls, and Abandoned calls.

The key to working with the Response Group Usage Report is to understand the difference between the reported call types:

- **Received calls.** Total number of calls received by all instances of the Response Group application.
- **Successful calls.** Total number of calls that were picked up by the Response Group application.
- **Offered calls.** Total number of calls that were transferred to a Response Group agent.
- **Answered calls.** Total number of calls that were actually answered by a Response Group agent.
- **Percentage of abandoned calls.** Percentage of calls that were received by the Response Group application but were never answered by an agent. This value is calculated by subtracting the Answered calls from the Received calls, and then dividing that value by the number of Received calls. For example, if you received 10 calls and 7 were answered, you would subtract 7 from 10, leaving 3 unanswered calls. That value would then be divided by 10, giving you an abandoned call percentage of 30%.
- **Transferred calls.** Total number of Response Group calls that were transferred because of a queue timeout or queue overflow.

If you are looking at the Response Group Usage Report and can't remember the definition for any of these call types, simply hold your mouse over the appropriate call type label. A tooltip will appear that offers a brief description of the call type.

The Response Group Usage Report allows you to filter on a workflow URI (the SIP address associated with that workflow). However, workflow URIs do not actually appear on the report itself. If you would like to know things such as which workflows are answering the most calls or which workflows are experiencing the most transferred calls, click the appropriate metric to open the Response Group Call List Report for that given time period. That reports does list the workflow URIs.

## Accessing the Response Group Usage Report

The Response Group Usage Report is accessed from the Monitoring Reports home page. You can drill down to the [Response Group Call List Report in Skype for Business Server](#) by clicking any of the following metrics:

- Received calls
- Successful calls
- Offered calls
- Answered calls
- Transferred calls

## Making the Best Use of the Response Group Usage Report

One of the more interesting uses of the Response Group Usage Report might not be readily apparent: the ability to retrieve usage information for a single Response Group workflow.

### Caution

A Response Group workflow is basically a set of instructions that determines what Skype for Business Server does when a user dials a particular phone number. To that end, each workflow is uniquely associated with a phone number. When someone calls that number, the workflow determines how the call will be handled. For example, the workflow might cause the call to be routed to a series of interactive voice response (IVR) questions that prompt the caller to enter additional information ("Press 1 for hardware support. Press 2 for software support.").

Alternatively, the workflow might cause the call to be placed in a queue, with the caller put on hold until an agent is available to answer the call. The availability of agents to answer calls is also dictated by the workflow: workflows are used to configure both business hours (the days of the week and the times of day when agents are available to answer calls) and holidays (days when no agents are available to answer calls). Any time you dial a phone number that belongs to the Response Group application you are essentially calling a Response Group workflow.

Although workflow URIs do not appear in the Response Group Usage Report, it's still possible to view the usage statistics for a single workflow, something that is often extremely useful. For example, suppose you recently unveiled a new ad campaign and are curious to know whether people are calling in to ask about that product. If you have associated a Response Group workflow with the phone number given in the ad campaign, you can easily check to see how many people (if any) are calling that number.

You might also use a similar approach to gauge the number of calls being handled by your internal help desk or your customer service department.

To review usage statistics for a particular workflow, enter the workflow URI in the Workflow URI box. Of course, as noted, workflow URIs (the SIP address associated with a workflow) do not appear on the report. That means you need to find some other way to determine the URI of a workflow. One way to do this is to use Windows PowerShell and the Skype for Business Server Management Shell. For example, this command returns the URIs for all your Response Group workflows:

```
Get-CsRgsWorkflow | Select-Object Name, PrimaryUri
```

That will return data similar to this:

Name	PrimaryUri
----	-----
Customer Support	sip:support@litwareinc.com
Help Desk	sip:helpdesk@litwareinc.com
New Ad Campaign	sip:newads@litwareinc.com

This command returns information for a single workflow, the one with the name New Ad Campaign:

```
Get-CsRgsWorkflow -Name "New Ad Campaign" | Select-Object Name, PrimaryUri
```

# Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Response Group Usage Report enables you to view data for all your Response Group workflows or to view data for an individual workflow. You can also choose how data should be grouped. In this case, usages are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Response Group Usage Report.

## Response Group Usage Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed.</p> <p>For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Workflow URI</b>	<p>Enables you to limit the returned data to the specified Response Group workflow. To use this filter, enter the Workflow SIP address. For example: sip:helpdesk@litwareinc.com</p>

# Metrics

The following table lists the information provided in the Response Group Usage Report.

## Response Group Usage Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Hourly</b> <b>Daily</b> <b>Weekly</b> <b>Monthly</b>	No	Indicates the selected time interval. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2015, you see an hourly breakdown of user registration activity for that date.
<b>Received calls</b>	No	Total number of calls received by all instances of the Response Group application. When you click this item, the report shows you the Response Group Call List report for the selected time period.
<b>Successful calls</b>	No	Total number of calls that were picked up the Response Group application. When you click this item, the report shows you the Response Group Call List report for the selected time period.
<b>Offered calls</b>	No	Total number of calls that were transferred to a Response Group agent. When you click this item, the report shows you the Response Group Call List report for the selected time period.
<b>Answered calls</b>	No	Total number of calls that were actually answered by a Response Group agent. When you click this item, the report shows you the Response Group Call List report for the selected time period.
<b>Percentage of abandoned calls</b>	No	Total number of calls that were received by the Response Group application but were never answered by an agent. This is calculated by subtracting the Answered calls from the Received calls, and then dividing that value by the number of received calls. For example, if you have 10 received calls and seven were answered, you would subtract seven from 10, leaving three unanswered calls. That value would then be divided by 10, giving you an abandoned call percentage of 30%.
<b>Average call minutes by agent</b>	No	Average amount of time a Response Group agent spent on a call.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Transferred calls</b>	No	Total number of Response Group calls that were transferred because of a queue timeout or queue overflow. When you click this item, the report shows you the Response Group Call List report for the selected time period.

# Response Group Call List Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Response Group application in Skype for Business Server.

The Response Group application provides a way for Skype for Business Server to answer and route phone calls based on the number that was dialed and, optionally, on the caller's responses to a series of questions. Typically, Response Group calls are not routed to an individual person but, instead, are routed to a team of people referred to as an agent group. For example, if someone calls the phone number for your help desk, Skype for Business Server can automatically route that call to the first available help desk agent. Alternatively, Skype for Business Server could ask a series of questions ("Press 1 if you are having hardware problems. Press 2 if you are having software problems. Press 3 if you are having network problems.") and then route the call to the most appropriate help desk agent based on the answer to those questions.

The Response Group Call List Report represents a collection of calls made for a specified period of time and for a specified type of call. The Response Group Usage Report (which must be opened first before you can open the Response Group Call List Report) recognizes the following call types:

- **Received calls.** Total number of calls received by all instances of the Response Group application.
- **Successful calls.** Total number of calls that were picked up by the Response Group application.
- **Offered calls.** Total number of calls that were transferred to a Response Group agent.
- **Answered calls.** Total number of calls that were actually answered by a Response Group agent.
- **Percentage of abandoned calls.** Percentage of calls that were received by the Response Group application but were never answered by an agent. This value is calculated by subtracting the Answered calls from the Received calls, and then dividing that value by the number of Received calls. For example, if you received 10 calls and 7 were answered, you would subtract 7 from 10, leaving 3 unanswered calls. That value would then be divided by 10, giving you an abandoned call percentage of 30%.
- **Transferred calls.** Total number of Response Group calls that were transferred because of a queue timeout or queue overflow.

## Accessing the Response Group Call List Report

The Response Group Call List Report can only be accessed by clicking one of the following metrics found on the [Response Group Usage Report in Skype for Business Server](#):

- Received calls
- Successful calls
- Offered calls
- Answered calls
- Transferred calls

## Making the Best Use of the Response Group Call List Report

The Response Group Call List Report allows you to limit the displayed data to calls involving a particular Response

Group workflow. To do that, you need to enter the workflow URI (the workflow's SIP address) in the Workflow URI box. Before you can do that, however, you must actually be able to see the Workflow URI box. To display the filtering options for the Response Group Call List Report, click the Show/Hide Parameters button in the upper left-hand portion of the report window.

Note that the Response Group Call List does not display information about either the Response code or the Diagnostic ID if you hold the mouse over either of those metrics. If you need more information, you might note the Response code and/or Diagnostic ID, and then search for those values in the [Top Failures Report in Skype for Business Server](#).

a question like this one: "Which individual workflow received the most calls?", you can do the following:

1. On the Response Group Usage Report, set the desired time period and then click the Received Calls metric. That will open the Response Group Call List Report.
2. Export the data shown on the Response Group Call List Report. For example, you might export the data in Microsoft Excel format, and then use Excel to convert that data to a comma-separated values file.
3. Run your analyses using Windows PowerShell.

For example, if you have saved the data to a file named C:\Data\Response\_Group\_Call\_List\_Report.csv, you can then use the following command to return the total number of received calls for each workflow listed in the report:

```
$calls = Import-Csv -Path "C:\Data\Response_Group_Call_List_Report.csv"
$calls | Group-Object Workflow | Select-Object Count, Name | Sort-Object Count -Descending
```

That will information similar to this:

Count	Name
160	Redmond Help Desk
47	Dublin Help Desk
31	North America Customer Support
16	EMEA Customer Support
14	Employment Opportunities

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Response Group Call List Report.

### Response Group Call List Report Filters

NAME	DESCRIPTION
<b>From</b>	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.



NAME	DESCRIPTION
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Workflow URI</b>	<p>Enables you to limit the returned data to the specified Response Group workflow. To use this filter, enter the Workflow SIP address. For example: sip:helpdesk@litwareinc.com</p>
<b>Calls</b>	<p>You can select one of the following call types:</p> <ul style="list-style-type: none"> <li>Received Calls</li> <li>Successful Calls</li> <li>Offered Calls</li> <li>Answered Calls</li> <li>Transferred Calls</li> </ul>

## Metrics

The following table lists the information provided in the Response Group Call List Report for each call received by the Response Group application.

### Response Group Call List Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Caller</b>	No	SIP address of the caller.
<b>Workflow</b>	No	SIP address of the Response Group workflow.
<b>Start time</b>	No	Date and time that the call started.
<b>End time</b>	No	Date and time that the call ended.
<b>Response code</b>	No	SIP response code sent when the session failed.
<b>Diagnostic ID</b>	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.

# IP Phone Inventory Report in Skype for Business Server

5/20/2019 • 7 minutes to read

**Summary:** Learn about the IP Phone Inventory Report in Skype for Business Server.

The IP Phone Inventory Report reports information about the IP phones currently in use in your organization. The IP Inventory Report provides a detailed list of the IP phones that were actually used during the specified reporting period. Among other things, this report lets administrators know if there are any old, outdated phones still in use that should be replaced; it can also alert administrators to the fact that there are expensive phones in the organization that are rarely being used. That type of information can be invaluable when it comes time to purchase new phones or to redistribute existing phones. (For example, a user who rarely uses his or her expensive phone might be asked to swap phones with a user who uses his or her phone much more frequently.)

It should be noted that this report does have a few limitations when it comes to being used as a true inventory report. For one thing, the IP Phone Report simply lists all the phones that logged on to Skype for Business Server during the specified time period, sorted by their last logon time. If a phone did not log on during the specified time period then it will not be listed in the inventory report. That includes phones that logged on before the time period started and were still logged on during the specified time interval. For example, suppose you wanted to look at all the phone inventory for July, 2015. Suppose, as well, that several phones logged on to Skype for Business Server on June 30, 2015, and were still logged on as of July 1st. Those phones will not show up on the inventory report for July 1st.

It's also important to note that the inventory report could include phones that your organization no longer uses. For example, suppose a number of Fabrikam phones logged on to the system on July 1, 2015; 5 days later your organization got rid of all those Fabrikam phones and replaced them with a newer Contoso model. The Fabrikam phones will still appear on the "inventory" report simply because they logged on to the system during the month of July.

In addition, the IP Phone Inventory Report does not report summary totals for the different types of phones. For example, suppose you have 105 Polycom CX600 phones. The report will not tell you that you have 105 of these phones; instead, you will simply see 105 separate entries for the Polycom Cx600. The only way to know that there are 105 entries for the Polycom Cx600 would be to count each of those entries manually.

## TIP

Or, export the data and use Microsoft Excel or Windows PowerShell to do that counting for you.

## Accessing the IP Phone Inventory Report

The IP Phone Inventory Report is accessed from the Monitoring Reports home page. If you click the User URI metric you can access the User Activity Report for that user. Clicking the Last activity metric for a peer-to-peer call will take you to the Peer-to-Peer Session Detail Report; clicking that same metric for a conference will take you to the Conference Detail Report.

## Making the Best Use of the IP Phone Inventory Report

If you're only interested in usage information for one particular kind of phone (for example, "How often are users using a Polycom CX600 phone?") you can get that information directly from the IP Phone Inventory Report by

filtering for that particular kind of phone. However, if you want summary information for all your phones (how many people are using a Polycom CX600, how many are using an LG-Nortel IP8540, etc.) then you will need to export the data and use another application (such as Windows PowerShell) to do that type of analysis. For example, suppose you export the data to a comma-separated values file (C:\Data\IP\_Phone\_Inventory\_Report.csv). In that case, you could use these two commands to provide summary data for all your phones:

```
$phones = Import-Csv "C:\Data\IP_Phone_Inventory_Report.csv"
$phones | Group-Object Manufacturer, "Hardware version" | Select-Object Count, Name | Sort-Object Count - Descending
```

That will return data similar to this:

Count	Name
-----	-----
267	POLYCOM, CX700
267	POLYCOM, CX600
166	POLYCOM, C
68	Microsoft, CPE
64	LG-Nortel, IP8540
59	Aastra, 6725ip
37	LG-Nortel, IP
22	POLYCOM, CX3000
11	Microsoft, CPE_A
9	POLYCOM, CX500
7	Aastra, 6721ip

Similarly, these two commands tell you which phones logged on to the system but were never actually used to make a call (the value of the Last activity metric is blank, indicating that there hasn't been any last activity):

```
$phones = Import-Csv "C:\Data\IP_Phone_Inventory_Report.csv"
$phones | Where-Object {$_.Last activity -eq ""}
```

That returns data similar to this for each phone that has not been used:

```
Manufacturer      : POLYCOM
Hardware version  : CX600
MAC address       : 00-04-F2-00-01-76
User URI          : 422
User agent        : CPE/4.0.7423.1 OPhone/4.0.7423.1 (Microsoft Lync 2010 (Beta) Phone Edition)
Last logon time   : 8/30/2010 4:44:48 PM
Last logoff time  : 8/30/2010 5:59:07 PM
Last activity     :
```

Another interesting way to use the IP Phone Inventory Report is this: if you have the MAC address of an IP Phone you can find out the user who last used that phone simply by entering that address in the MAC address text box. The IP Phone Inventory report will then report back (among other things) the SIP address of the user who last logged on with that phone. Alternatively, you can enter a user SIP address (in the User URI prefix box) to find out all the phones that have been used by that user.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the IP Phone Inventory enables you to view only the phones manufactured by a specific company, or even a specific version of those phones. You can also choose how data should be grouped. In this case, registrations are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the IP Phone Inventory Report.

### IP Phone Inventory Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Manufacturer</b>	<p>Name of the company that manufactured the IP phone. The values for this filter are automatically populated for you based on the IP phones that are currently in the database.</p>
<b>Hardware version</b>	<p>Version number of the IP phone; by using the Manufacturer and the Hardware version filters you can uniquely identify a particular type of phone. The values for this filter are automatically populated for you based on the IP phones that are currently in the database.</p>
<b>User agent</b>	<p>Identifier for the software used by the IP phone. The values for this filter are automatically populated for you based on the IP phones currently in the database.</p>
<b>MAC address</b>	<p>Unique identifier for the network interface on the IP phone. The Media Access Control (MAC) address is typically assigned at the time the phone is manufactured and is hard-wired into the device hardware.</p> <p>To search for records pertaining to a specific MAC address simply enter that address. For example: 00-08-5D-16-16-48</p> <p>You must enter the complete address. A partial address (for example 00-08-5D) does not return any data.</p>
<b>Last activity before days</b>	<p>Select one of the following values: [All] 10 20 30</p>

NAME	DESCRIPTION
<b>Last logoff time before days</b>	Select one of the following values: [All] 10 20 30
<b>User URI prefix</b>	SIP address of the user who used the IP phone.

## Metrics

The following table lists the information provided in the IP Phone Inventory Report.

### IP Phone Inventory Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Manufacturer</b>	Yes	Name of the company that manufactured the IP phone.
<b>Hardware version</b>	Yes	Version number of the IP phone.
<b>MAC address</b>	Yes	Unique identifier for the network interface on the IP phone. The MAC address is typically assigned at the time the phone is manufactured and is hard-wired into the device hardware.
<b>User URI</b>	Yes	SIP address of the user who used the IP phone.
<b>User agent</b>	Yes	Identifier for the software used by the IP phone.
<b>Last logon time</b>	Yes	Date and time that the IP phone last logged on to Skype for Business Server.
<b>Last logoff time</b>	Yes	Date and time that the IP phone last logged off from Skype for Business Server.
<b>Last activity</b>	Yes	Date and time that the IP phone was last used.

# Call Admission Control Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Call Admission Control Reports used in Skype for Business Server.

The Call Admission Control Report provides information about peer-to-peer and conferencing sessions that were conducted under restrictions set in place by Call Admission Control. Call Admission Control provides a way for administrators to allow (or not allow) communication sessions based on bandwidth constraints. For example, administrators can create policies that impose a limit on the amount of bandwidth available for voice and video calls. If that bandwidth limit has been reached, then no new voice or video calls can be placed until one of the current calls has ended and freed up the required network resources.

## Accessing the Call Admission Control Report

The Call Admission Control Report is accessed from the Monitoring Reports home page. From the Call Admission Control Report you can drill down to either of the following reports:

- Conference Detail Report - To access this report, click the Details metric from a conference session.
- Peer-to-Peer Session Detail Report - To access this report, click the Details metric for a peer-to-peer session.

## Making the Best Use of the Call Admission Control Report

To get a list of calls that failed because of insufficient bandwidth, select Calls rejected because of call admission control from the Call category dropdown list. Most of the returned calls will likely have a diagnostic ID of 5:

Insufficient bandwidth to establish session. Attempt PSTN re-route.

That indicates that Call Admission Control limitations were preventing the call from being made on the VoIP network.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Call Admission Control Report enables you to filter calls by the user who initiated the call or by the user who was being called. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Call Admission Control Report.

### Call Admission Control Report Filters

NAME	DESCRIPTION
------	-------------

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/17/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/17/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Pool</b>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>
<b>Activity type</b>	<p>Type of activity. Select one of the following activities: [All] Peer-to-Peer Conference</p>
<b>Call category</b>	<p>Indicates the reason that CAC was used for the call. Select one of the following: [All] Call rejected because of call admission control Calls rerouted through PSTN because of call admission control</p>

## Metrics for Peer-to-Peer Sessions

The following table lists the information provided in the Call Admission Control Report for peer-to-peer sessions (that is, sessions involving just two participants).

### Metrics for Peer-to-Peer Sessions

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Detail</b>	No	When you click this item, the report shows you a Peer-to-Peer Session Detail Report for the specified session.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>From user</b>	Yes	SIP address of the user who initiated the session.
<b>To user</b>	Yes	SIP address of the user who was invited to join the session.
<b>Modalities</b>	Yes	Communication modalities (such as audio and video) that were used during the session.
<b>Invite time</b>	Yes	Date and time the initial session invitation was sent to the From user.
<b>Response time</b>	Yes	Date and time that the invitation acceptance was received.
<b>End time</b>	Yes	Date and time that the session ended.
<b>Diagnostic ID</b>	Yes	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

## Metrics for Conferencing Sessions

The following table lists the information provided in the Call Admission Control Report for conferencing sessions (that is, sessions involving three or more participants).

### Metrics for Conferencing Sessions

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Conference URI</b>	Yes	Unique identifier for the conference. When you click this item, the report shows the individual conference participants.
<b>Organizer</b>	Yes	SIP address of the user who organized the conference.
<b>Pool</b>	Yes	Edge Server used in the conference.
<b>Start time</b>	Yes	Date and time that the conference started.
<b>End time</b>	Yes	Date and time that the conference ended.



# Metrics for Individual Conference Participants

The following table lists the information provided in the Call Admission Control Report for individual conference participants.

## Metrics for Individual Conference Participants

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Role</b>	No	Role (for example, Presenter) played by the conference participant.
<b>Participant</b>	No	SIP address of the conference participant.
<b>Connectivity</b>	No	Network connectivity (typically From Internal or From External) for the participant.
<b>Modality</b>	No	Conference type (for example, A/V conferencing).
<b>Join time</b>	No	Date and time that the participant joined the conference.
<b>Leave time</b>	No	Date and time that the participant left the conference.
<b>Diagnostic ID</b>	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

# Peer-to-Peer Session Detail Report in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Peer-to-Peer Session Detail Report in Skype for Business Server.

The Peer-to-Peer Session Detail Report returns detailed information about a peer-to-peer session. For example, if you select an instant messaging session, the report will tell you the number of messages sent by each of the two users in the session.

## Accessing the Peer-to-Peer Session Detail Report

The Peer-to-Peer Session Detail Report can be accessed from any of the following reports (all of which can be accessed from the Monitoring Reports home page):

- IP Phone Inventory Report
- User Activity Report
- Call Admission Control Report
- Failure List Report

From within the Peer-to-Peer Session Detail Report you can access the [Diagnostic Report in Skype for Business Server](#) by clicking the Diagnostic Report (Details) metric. You can also access the Top Failures Report by clicking either of these two metrics:

- Response
- Diagnostic ID

## Making the Best Use of the Peer-to-Peer session Detail Report

The Peer-to-Peer Session Detail Report includes a large number of metrics, many of which might not be familiar to system administrators. Often-times, however, you can view a tooltip that offers a brief description of that metric simply by holding your mouse over the metric label.

Note that the actual metrics shown on a given report will depend on the type of peer-to-peer session you selected. An audio/video session will report a different set of metrics than an instant messaging session.

You can also hold your mouse over the Response code and Diagnostic ID metrics in order to obtain a description of those values:

## Filters

None. You cannot filter the Peer-to-Peer Session Detail Report.

## Session Information Metrics

The following table lists the information provided in the Peer-to-Peer Session Detail Report for each session.

### Session Information Metrics

<b>NAME</b>	<b>DESCRIPTION</b>
<b>Pool FQDN</b>	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server involved in the session.
<b>Invite time</b>	Date and time the session invitation was originally sent.
<b>Response time</b>	Date and time that the invitation acceptance was received.
<b>From user</b>	SIP address of the user who initiated the session.
<b>From user agent</b>	Software used by the endpoint of the user who initiated the session.
<b>Is From user internal</b>	Indicates whether the user who initiated the session was logged on to the internal network.
<b>Is From user integrated with desk phone</b>	Indicates whether the endpoint used by the user who initiated the session is integrated with his or her desktop phone.
<b>Session Priority</b>	Priority assigned to the session. Valid priorities are: Unknown; Non-Urgent; Normal; Urgent; and Emergency.
<b>Response code</b>	SIP response code sent when the session failed.
<b>Front end</b>	Name of the Front End Server used in the conference.
<b>Capture time</b>	Date and time that the session information was recorded.
<b>End time</b>	Date and time the session ended.
<b>To user</b>	SIP address of the user who was invited to the session.
<b>To user agent</b>	Software used by the endpoint of the user who was invited to the session.
<b>Is To user internal</b>	Indicates whether the user who was invited to the session was logged on to the internal network.
<b>Is To user integrated with desk phone</b>	Indicates whether the endpoint used by the user who was invited to the session is integrated with his or her desktop phone.
<b>Is retried session</b>	Indicates whether the session is an attempt to retry a session that previously failed.
<b>Diagnostic ID</b>	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Hold the mouse over the ID number to view additional information about that ID.

## Metrics for Modalities

The following table lists the information provided in the Peer-to-Peer Session Detail Report for each session modality.

## Metrics for Modalities

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Modalities</b>	No	Modalities used in the session. For example, instant messaging (IM) or file transfer.
<b>From user messages</b>	No	Number of messages sent by the user who initiated the session.
<b>To user messages</b>	No	Number of messages sent by the user who was invited to join the session.

## Metrics for Diagnostic Reports

The following table lists the information provided in the Peer-to-Peer Session Detail Report for each diagnostic report.

### Metrics for Diagnostic Reports

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Detail</b>	No	When you click this item, the report shows the Diagnostic Report for the session.
<b>Report time</b>	No	Date and time the report was recorded.
<b>Request</b>	No	SIP request type. For example, INVITE or BYE.
<b>Diagnostic ID</b>	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
<b>Content type</b>	No	Type of media content used in the conference. For example, a common content type is Application/sdp. Session Description Protocol (SDP) is a standard Internet protocol used for session announcements, session invitations, and other forms of multimedia session initiation.
<b>Reported by</b>	No	Computer (that is, client or server) that reported the problem.

# Call Diagnostic Reports (per user) in Skype for Business Server

5/20/2019 • 9 minutes to read

The Call Diagnostic Reports provide per-user information about failed peer-to-peer and conferencing sessions. At this time there is only one report, the **User Activity Report**.

The User Activity Report provides a detailed list of the peer-to-peer and conferencing sessions carried out by your users in a given time period. Unlike many of the Monitoring Reports, the User Activity Report ties each call to individual users. For example, peer-to-peer sessions specify the SIP URIs of the person who initiated the call (the From user) and the person who was being called (the To user). If you expand the information for a conference, you'll see a list of all the conference participants and the role they held for that conference.

The User Activity Report is sometimes referred to as the "help desk" report. That's because the report is often used by help desk personnel to retrieve session information for a specific user. You can filter for calls made to or made by an individual user simply by typing the user's SIP URI in the User URI prefix box.

If you do this, the User Activity Report will return information for any user whose SIP URI begins with the specified string. For example, if you type **ken** in the URI box, the User Activity Report will locate **Ken.Myer@litwareinc.com**. However, it will also locate these users:

- **ken** azi@litwareinc.com
- **ken** burg@litwareinc.com
- **Ken**.Sanchez@litwareinc.com
- **Ken** nedy@litwareinc.com

To ensure that information only for Ken Myer is returned, either type his full URI (Ken.Myer@litwareinc.com) in the search box or at least enough type of Ken's URI to uniquely distinguish him from other users in your organization. For example:

Ken.my

## To access the user activity report

The User Activity Report is accessed from the Monitoring Reports home page. You can also reach the User Activity Report by clicking the User URI metric on the [IP Phone Inventory Report in Skype for Business Server](#). From within the User Activity Report, clicking the Conference URI (for a conference) takes you to the Conference Detail Report. Similarly, clicking the Detail metric for a peer-to-peer call takes you to the [Peer-to-Peer Session Detail Report in Skype for Business Server](#).

## Making the best use of the user activity report

Although there is a lot of good information in the User Activity Report, that information can sometimes be difficult to locate. For example, all the user activity that takes place in your organization during a specified period is included in the User Activity Report; that means that, buried, within the report is information about which users actually used Skype for Business Server in some way.

## NOTE

Technically, it's possible that some user activity might go unrecorded: while Skype for Business Server strives to keep information about all phone calls it's possible that a call could have been made without the information about that call being written to the database. Skype for Business Server is designed to give an extremely accurate but not necessarily perfect look at how Skype for Business Server is being used. (The fact that there is no guarantee that 100% of all calls are recorded explains why Skype for Business Server monitoring should not be used as a billing system.) Second, a Monitoring Report can only display, at most, 1,000 records. Depending on the amount of user activity you have, and depending on the time period you are working with, that means your query might not return all the data actually stored in the database.

- Which users actually used the system during this time period?
- Which of my users were the most active during this time period?
- Are the users who make the most phone calls also the users who participate in the most instant messaging sessions?

If you need to answer questions like this, you can export the data retrieved by the Monitoring Reports to an Excel spreadsheet. You then use that spreadsheet and/or a comma-separated values file to analyze the data in ways that the User Activity Report. For example, suppose you have exported the report data to Excel and then to a comma-separated values file. At that point, you can import the data from the .CSV file to Windows PowerShell by using a command similar to this:

```
$x = Import-Csv -Path "C:\Data\User_Activity_Report.csv"
```

After the data has been imported you can then use simple Windows PowerShell commands to help answer your questions. For example, this command returns a list of unique users who served as the "From user" in at least one session:

```
$x | Group-Object "From user" | Select Name | Sort-Object Name
```

In other words:

```
Name
----
David.Ahs@litwareinc.com
Gilead.Amosnino@litwareinc.com
Henrik.Jensen@litwareinc.com
Ken.Myer@litwareinc.com
Pilar.Ackerman@litwareinc.com
```

This command lists the unique users (based on the total number of sessions that they participated in:

```
$x | Group-Object "From user" | Select Count, Name | Sort-Object Count -Descending
```

That returns data similar to this:

Count	Name
-----	----
523	Ken.Myer@litwareinc.com
63	David.Ahs@litwareinc.com
29	Pilar.Ackerman@litwareinc.com
17	Gilead.Amosnino@litwareinc.com
10	Henrik.Jensen@litwareinc.com

This command limits the reported sessions to those that included audio as a modality:

```
$x | Where-Object {$_.Modalities -match "audio"} | Group-Object "From user" | Select Count, Name | Sort-Object Count -Descending
```

If you hold your mouse over any Diagnostic ID shown on the report, a tooltip will appear describing that ID.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the User Activity Report enables you to filter the returned data based on such things as activity type (that is, peer-to-peer sessions or conferencing sessions) or by the user's SIP address (allowing you to view the activities for one user). You can also choose how data should be grouped. In this case, usages are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the User Activity Report.

### User activity report filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/17/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/17/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>Activity type</b>	Type of activity. Select one of the following: [All] Peer-to-peer Conference
<b>Modality</b>	The Modality available to you varies depending on the select Activity Type. If the Activity Type is Peer-to-Peer, you can select IM; File Transfer; Application Sharing; Voice; or Video as the modality. If the Activity Type is Conference, you can select IM Phone conference; Web conference; Application Sharing; Voice/Video conference; or Telephony conference.
<b>Session category</b>	Indicates whether the activity in question succeeded or failed. Select one of the following: [All] Success Expected failure Unexpected failure An "expected failure" is a failure that is expected to happen; for example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail. An "unexpected failure" is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
<b>User URI prefix</b>	SIP address for the user. To view records only for the user Ken Myer you need to enter Ken Myer's SIP address. For example: sip:kenmyer@litwareinc.com

## Metrics for peer-to-peer sessions

The following table lists the information provided in the User Activity Report for peer-to-peer sessions (that is, sessions involving just two participants).

### Metrics for peer-to-peer sessions

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Detail</b>	No	When you click this item, the report shows you the Peer-to-Peer Session Detail Report for the selected session.
<b>From user</b>	Yes	SIP address of the user who initiated the peer-to-peer session.
<b>To user</b>	Yes	SIP address of the user who joined the peer-to-peer session.
<b>Modalities</b>	Yes	Type of communication used in the session. For example, IM, audio, or file transfer.
<b>Invite time</b>	Yes	Date and time the initial invitation to join the peer-to-peer session was sent.



NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Response time</b>	Yes	Date and time that the "To" user accepted the session invitation.
<b>End time</b>	Yes	Date and time the peer-to-peer session ended.
<b>Diagnostic ID</b>	Yes	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

## Metrics for conferencing sessions

The following table lists the information provided in the User Activity Report for conferencing sessions (that is, sessions involving three or more participants).

### Metrics for conferencing sessions

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Conference URI</b>	Yes	Unique conference identifier. When you click this item, the report shows you the Conference Detail Report for the selected session. When you expand this item, the report shows you information about the conference participants. For details, see the "Metrics for Conference Participants" section later in this topic.
<b>Organizer</b>	Yes	SIP address of the user who organized the conference.
<b>Pool</b>	Yes	Name of the Edge Server (if any) used in the conference.
<b>Start time</b>	Yes	Date and time that the conference began.
<b>End time</b>	Yes	Date and time that the conference ended.

## Metrics for conference participants

The following table lists the information provided in the User Activity Report provides for each participant in a conference.

### Metrics for conference participants

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Role</b>	No	Conference role (for example, Presenter) for the user.
<b>Participant</b>	No	SIP address of the user.
<b>Connectivity</b>	No	Network connection type. For example "From Internal" for internal connection or "From PSTN" for dial-in users.
<b>Join time</b>	No	Date and time that the user joined the conference.
<b>Leave time</b>	No	Date and time that the user left the conference.
<b>Diagnostic ID</b>	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

# Call Diagnostic Reports in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the multi-user Call Diagnostic Reports used in Skype for Business Server.

The Call Diagnostic Reports provide summary information and diagnostic data for failed peer-to-peer and conferencing sessions.

## In this section

- [Call Diagnostic Summary Report in Skype for Business Server](#) Provides an overall summary of failed peer-to-peer sessions and conference sessions. Peer-to-peer sessions are sessions that involve just two participants. Conferencing sessions involve three or more participants.
- [Peer-to-Peer Activity Diagnostic Report in Skype for Business Server](#) Provides an overall trend view of failed peer-to-peer sessions. A peer-to-peer session involves just two participants.
- [Conference Diagnostic Report in Skype for Business Server](#) Provides an overall trend view of failed conferencing sessions and trend views for each conference modality. Conferencing sessions involve at least three participants.
- [Top Failures Report in Skype for Business Server](#) Provides a list of the most frequent failures and their trends over time.
- [Failure Distribution Report in Skype for Business Server](#) Provides an analysis of failed sessions.
- [Failure List Report in Skype for Business Server](#) Provides detailed information about the individual participants involved in a failed conference.
- [Diagnostic Report in Skype for Business Server](#) Provides diagnostic and troubleshooting information (including SIP response codes and diagnostic headers and IDs) for failed sessions.

# Call Diagnostic Summary Report in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Call Diagnostic Summary Report used in Skype for Business Server.

The Call Diagnostic Summary Report provides an overall look at failed peer-to-peer and conferencing sessions. The report shows the overall failure rate for both types of sessions, and further breaks the failure information down by session modality type:

- Instant messaging
- Application sharing
- File transfer
- Audio
- Video

## Accessing the Call Diagnostic Summary Report

The Call Diagnostic Summary Report is accessed from the Monitoring Reports Home page. From the Call Diagnostic Summary Report you can access the [Peer-to-Peer Activity Diagnostic Report in Skype for Business Server](#) by clicking the Failure rate metric under the Peer-to-Peer Session Summary section of the report. You can also access the [Conference Diagnostic Report in Skype for Business Server](#) by clicking any of the following conference metrics:

- Overall session failure rate
- Focus failure rate
- MCU failure rate

## Making the Best Use of the Call Diagnostic Summary Report

The Call Diagnostic Summary Report includes graphs that compare failure rates for the various modalities used in Skype for Business Server. The columns in these graphs are actually hotlinks; for example, if you click the Instant messaging column for peer-to-peer sessions, you'll drill down to an instance of the [Peer-to-Peer Activity Diagnostic Report in Skype for Business Server](#), a report that provides additional details about all the instant messaging sessions included in the Call Diagnostic Summary Report.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Call Diagnostic Summary Report enables you to filter on such things as the Registrar pool or Edge Server used in the session. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Call Diagnostic Summary Report.

### Call Diagnostic Summary Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Pool</b>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>

## Metrics for Peer-to-Peer Sessions

The following table lists the information provided in the Call Diagnostic Summary Report for peer-to-peer sessions (that is, sessions involving just two participants).

### Metrics for Peer-to-Peer Sessions

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Total sessions</b>	No	Total number of peer-to-peer sessions conducted.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Failure rate</b>	No	Percentage of peer-to-peer sessions that failed. When you click this item, the report shows the Peer-to-Peer Activity Diagnostic report, which displays more detailed information about the failed peer-to-peer sessions.

## Metrics for Conferencing Sessions

The following table lists the information provided in the Call Diagnostic Report for conferencing sessions (that is, sessions involving three or more participants).

### Metrics for Conferencing Sessions

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Total conferences</b>	No	Total number of conferences conducted.
<b>Total conference sessions</b>	No	Total number of conferencing sessions conducted.
<b>Overall session failure rate</b>	No	Percentage of the total conferencing sessions that failed.
<b>Focus sessions</b>	No	Total number of Focus-based conferencing sessions that failed.
<b>Focus failure rate</b>	No	Percentage of the Focus-based conferencing sessions that failed.
<b>MCU sessions</b>	No	Total number of conferencing server-based (formerly known as Multipoint Control Unit or MCU) conferences that failed.
<b>MCU failure rate</b>	No	Percentage of the conferencing server-based (formerly known as Multipoint Control Unit or MCU) conferences that failed.

# Conference Summary Subreport in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Conference Summary Subreport in Skype for Business Server.

The Conference Summary Subreport provides an overall view of failed conference sessions. These failed sessions are further broken down by session type: Focus sessions and MCU sessions.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Conference Summary Subreport.

### Conference Summary Subreport Filters

NAME	DESCRIPTION
<b>From</b>	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.
<b>To</b>	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.
<b>Pool</b>	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.

## Metrics

The following table lists the information provided in the Conference Summary Subreport.

## Conference Summary Subreport Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Total conferences</b>	No	Total number of conferences held.
<b>Total conference sessions</b>	No	Total number of conference sessions. A single conference can have multiple sessions; for example, a conference might include both a Focus session and an MCU session.
<b>Overall session failure rate</b>	No	Percentage of all conferences that failed.
<b>Focus sessions</b>	No	Total number of Focus sessions.
<b>Focus failure rate</b>	No	Percentage of Focus sessions that failed.
MCU sessions	No	Total number of MCU sessions.
<b>MCU failure rate</b>	No	Percentage of MCU sessions that failed.
<b>MCU sessions by modality</b>	No	Total number of MCU sessions, grouped by modality (for example, IM conferencing).
<b>Failure rate by modality</b>	No	Percentage of MCU sessions that failed, grouped by modality (for example, IM conferencing).



# P2P Summary Subreport in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the P2P Summary Subreport in Skype for Business Server.

The P2P Summary Subreport provides an overall view of your failed peer-to-peer communication sessions.

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the P2P Summary Subreport.

### P2P Summary Subreport Filters

NAME	DESCRIPTION
<b>From</b>	Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.
<b>To</b>	End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.
<b>Pool</b>	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.

## Metrics

The following table lists the information provided in the P2P Summary Subreport.

### P2P Summary Subreport Metrics

<b>NAME</b>	<b>CAN YOU SORT ON THIS ITEM?</b>	<b>DESCRIPTION</b>
<b>Total sessions</b>	No	Total number of sessions, including successful sessions, failed sessions (both expected failures and unexpected failures), and uncategorized sessions.
<b>Failure rate</b>	No	Percentage of peer-to-peer sessions that failed.
<b>Sessions by Modality</b>	No	Total number of sessions grouped by modality (for example, instant messaging).
<b>Failure rate by modality</b>	No	Total number of failed sessions grouped by modality (for example, instant messaging).

# Peer-to-Peer Activity Diagnostic Report in Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Learn about the Peer-to-Peer Activity Diagnostic Report in Skype for Business Server.

The Peer-to-Peer Activity Diagnostic Report provides information about the success and failure of your peer-to-peer communication sessions. Note that Skype for Business Server distinguishes between different kinds of failure:

- **Expected failure.** An expected failure is typically a failure only in the most technical sense. For example, suppose you call someone, but he or she is away from the office and is unable to answer the phone. Because the call was not answered, the call is technically considered a failure. On the other hand, this was an expected failure: Skype for Business Server does not expect you to answer the phone if you're not available to answer the phone. Likewise, an expected failure will occur if you attempt to send an instant message to a user who is offline, or is logged on only to a phone that does not support instant messaging.
- **Unexpected failure.** An unexpected error is exactly what the name implies: an error that, based on the circumstances, you would not expect to occur. For example, suppose you call someone and that person is available to answer the call; however, when Skype for Business Server tries to route your call to voice mail the call fails because connectivity to Exchange Unified Messaging has been lost. That's an unexpected error: you would expect that calls could always be routed to voice mail. As a general rule, unexpected failures are true failures: they are problems that likely cannot be remedied through user education or similar measures.

Note that the Success, Expected failure, and Unexpected failure metrics might not add up to the Total sessions metric. For example, in the preceding illustration, we have the following values:

SUCCESSES	EXPECTED FAILURES	UNEXPECTED FAILURES	TOTAL SESSIONS
2024	469	16	2521

If you add 2024 + 469 + 16 you get a total of 2,509 sessions, yet the Total sessions column shows a total of 2,521 sessions. The "missing" 12 sessions are sessions that the system was unable to categorize as successful or unsuccessful. That will sometimes be the case when a third-party product introduces a new diagnostic code that is unfamiliar to Skype for Business Server. When that happens, calls made using that product, and reporting that diagnostic code, cannot always be categorized as being a Success, an Expected failure, or an Unexpected failure.

## Accessing the Peer-to-Peer Activity Diagnostic Report

The Peer-to-Peer Diagnostic Report is accessed from the Monitoring Reports home page. You can access the [Failure Distribution Report in Skype for Business Server](#) by clicking either of the following metrics:

- Unexpected failure volume
- Expected failure volume

## Making the Best Use of the Peer-to-Peer Activity Diagnostic Report

There are a number of ways you can filter the Peer-to-Peer Activity Diagnostic Report but, by default, those filtering options are hidden from view. To view the filtering options available to you, click the Show/Hide Parameters button in the upper right-hand corner of the report window. Once you do that the filtering options will

be available for use.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Peer-to-Peer Activity Diagnostic Report enables you to filter on such things as the session modality (for example, instant messaging, file transfer, or application sharing). You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Peer-to-Peer Activity Diagnostic Report.

### Peer-to-Peer Activity Diagnostic Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Pool</b>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>

NAME	DESCRIPTION
<b>Modality</b>	Indicates the type of communication activity that took place. Select one of the following: [All] Instant messaging File transfer Application sharing Audio Video

## Metrics (per modality)

The following table lists the information provided in the Peer-to-Peer Activity Diagnostic Report for each modality.

### Metrics (per modality)

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Success volume</b>	No	Total number of successful peer-to-peer sessions.
<b>Success percentage</b>	No	Percentage of peer-to-peer sessions that completed with significant problems. Calculated by dividing the Success volume by the Total sessions.
<b>Expected failure volume</b>	No	Total number of sessions where an "expected failure" occurred. An expected failure is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail.
<b>Expected failure percentage</b>	No	Percentage of peer-to-peer sessions that experienced an expected error. Calculated by dividing the Expected failure volume by the Total sessions.
<b>Unexpected failure volume</b>	No	Total number of sessions where an "unexpected failure" occurred. An unexpected failure is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
<b>Unexpected failure percentage</b>	No	Percentage of peer-to-peer sessions that experienced an unexpected error. Calculated by dividing the Unexpected failure volume by the Total sessions.
<b>Total sessions</b>	No	Total number of sessions, including successful sessions, failed sessions (both expected failures and unexpected failures), and uncategorized sessions.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
------	----------------------------	-------------

# Conference Diagnostic Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Conference Diagnostic Report used in Skype for Business Server.

The Conference Diagnostic Report provides information about the success and failure of all conferencing sessions. Note that Skype for Business Server distinguishes between different kinds of failure:

- **Expected failure.** An expected failure is typically a failure only in the most technical sense. For example, suppose someone starts a conference but hangs up before anyone can join. Technically that's a failure: the conference was initiated, but not completed. However, that's a failure that you would expect to happen: if the organizer cancels the conference before anyone can join then you would not expect that conference to be completed.
- **Unexpected failure.** An unexpected error is exactly what the name implies: an error that, based on the circumstances, you would not expect to occur. For example, suppose a conference could not be held because the organizer's meeting policy could not be retrieved. That's an unexpected error: after all, you should always be able to retrieve a user's meeting policy.

Note that the Success, Expected failure, and Unexpected failure metrics might not add up to the Total sessions metric. For example, you might see the following values in the Report:

SUCCESSES	EXPECTED FAILURES	UNEXPECTED FAILURES	TOTAL SESSIONS
2024	469	16	2521

If you add 2024 + 469 + 16 you get a total of 2,509 sessions and yet, the Total sessions column shows a total of 2,521 sessions. The "missing" 12 sessions are sessions that the system was unable to categorize as successful or unsuccessful. That will sometimes be the case when a third-party product introduces a new diagnostic code that is unfamiliar to Monitoring Server. When that happens, calls made using that product, and reporting that diagnostic code, cannot always be categorized as being a Success, an Expected failure, or an Unexpected failure.

## Accessing the Conference Diagnostic Report

The Conference Diagnostic Report is accessed from the Monitoring Reports home page. You can access the [Failure Distribution Report in Skype for Business Server](#) by clicking either of the following metrics:

- Unexpected failure volume
- Expected failure volume

## Making the Best Use of the Conference Diagnostic Report

The Conference Diagnostic Report includes a series of graphs. Each of the columns shown in the graph is actually a hyperlink. If you click a column, you'll drill down to the [Failure Distribution Report in Skype for Business Server](#) for that time period and that conference type.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different

ways. For example, the Conference Diagnostic Report enables you to filter on such things as the type of conference being conducted (for example, a Focus-based conference) or by the Edge Server used in the conference. You can also choose how data should be grouped. In this case, conferences are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Conference Diagnostic Report.

### Conference Diagnostic Report Filters

NAME	DESCRIPTION
<p><b>From</b></p>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<p><b>To</b></p>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<p><b>Interval</b></p>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed) Monthly (a maximum of 12 months can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<p><b>Pool</b></p>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>



NAME	DESCRIPTION
<b>Conference sessions</b>	Indicates the type of conferencing session. Select one of the following: [All] Focus sessions All MCU sessions IM conferencing Application sharing A/V conferencing

## Metrics

The following table lists the information provided in the Conference Diagnostic Report for each type of conferencing session.

### Conference Diagnostic Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Success volume</b>	No	Total number of successful conferences.
<b>Success percentage</b>	No	Percentage of conferences that completed with significant problems. Calculated by dividing the Success volume by the Total sessions.
<b>Expected failure volume</b>	No	Total number of conferences where an "expected failure" occurred. An expected failure is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail.
<b>Expected failure percentage</b>	No	Percentage of conferences that experienced an expected error. Calculated by dividing the Expected failure volume by the Total sessions.
<b>Unexpected failure volume</b>	No	Total number of conferences where an "unexpected failure" occurred. An unexpected failure is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
<b>Unexpected failure percentage</b>	No	Percentage of conferences that experienced an unexpected error. Calculated by dividing the Unexpected failure volume by the Total sessions.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Total sessions</b>	No	Total number of conferences, including successful conferences, failed conferences (both expected failures and unexpected failures), and uncategorized conferences.

# Top Failures Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Top Failures Report in Skype for Business Server.

The Top Failures Report provides a look at the most-commonly reported failures and their trends over time. Failures are based on a combination of the following two metrics:

- **Diagnostic ID.** Unique identifier (in the form of an ms-diagnostics header) that is attached to a SIP message. Diagnostic IDs provide information useful in troubleshooting call-related problems.
- **Response code.** Response codes are used in SIP communication sessions to respond to SIP requests. For example, suppose Ken sends the INVITE request to Pilar Ackerman (that is, suppose Ken Myer calls Pilar Ackerman). If Pilar answers, her phone will send the response code 200 (OK), letting Ken's phone know that Pilar has answered. The Top Failures Report only includes response codes that were sent in response to a call failure; Skype for Business Server does not keep track of all the response codes issued during the course of a call.

Information is reported not only for the total number of sessions where a failure occurred but also for the total number of users who were impacted by the failure.

## Accessing the Top Failures Report

The Top Failures Report is accessed from the Monitoring Reports home page. Clicking the Reported sessions metric will take you to the [Failure Distribution Report in Skype for Business Server](#).

## Making the Best Use of the Top Failures Report

The Top Failures Report is unusual in one regard: it allows you to filter on as many as 5 diagnostic IDs at once. (Typically you can only filter on one item - such as one user SIP address - at a time.) To filter on multiple diagnostic IDs, simply enter each ID in the Diagnostic IDs box, separating the IDs by using commas. (If you want to, you can leave a blank space after each comma.) For example:

1011, 2412, 1033, 52116, 1008

Do that, and only failed calls that reported at least one of those five diagnostic IDs will be displayed.

If you hold your mouse over a Response code you'll see a tooltip that tells you what the Response code in question means. For example, if you hold the mouse over the Response code 486 you'll see this message:

Busy Here.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Top Failures Report enables you to filter the returned data based on such things as the activity type (peer-to-peer session or conferencing session) or by the SIP response code that accompanied the failed session. You can also choose how data should be grouped. In this case, usages are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Top Failures Report.

### Top Failures Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Activity type</b>	<p>Type of activity. Select one of the following: [All] Peer-to-peer Conference</p>
<b>Modality</b>	<p>At this time the only option available is <b>[All]</b>.</p>
<b>Pool</b>	<p>Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.</p>
<b>Category</b>	<p>Type of failure experienced. Select one of the following: Both expected and unexpected failure Unexpected failure</p> <p>An "expected failure" is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail. An "unexpected failure" is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.</p>
<b>Response code</b>	<p>SIP response code sent when the conference failed. Enter the entire response code For example: 400</p>

NAME	DESCRIPTION
<b>Diagnostic ID</b>	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

## Metrics

The following table lists the information provided in the Top Failures Report.

### Top Failures Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	Yes	Relative rank based on the number of reported sessions.
<b>Reported sessions</b>	Yes	Total number of failed sessions based on diagnostic ID and SIP response code.
<b>Users impacted</b>	Yes	Total number of users affected by the failed session.
<b>Failure information</b>	No	Detailed information about the failure, including diagnostic ID, SIP response code, and description of why the session failed.
<b>Trend in the past</b>	No	Graphs failed sessions over time.

# Failure Distribution Report in Skype for Business Server

5/20/2019 • 7 minutes to read

**Summary:** Learn about the Failure Distribution Report in Skype for Business Server.

The Failure Distribution Report ranks failed sessions in the following categories:

- Top diagnostic reasons
- Top modalities
- Top pools
- Top sources
- Top components
- Top from users
- Top to users
- Top from user agents

You can use these categories to determine exactly where a problem is occurring and, in some cases, why the problem is occurring. For example, suppose you recorded 242 failed audio/video sessions during a given day. If you look at the Failure Distribution Report, it might show that 237 of those failed sessions took place in your Dublin pool. That gives you a good place to start when it comes to tracking down and diagnosing the causes behind those failures. If you click on the Dublin pool under the **Top pools** category, you will see a Failure Distribution Report just for that pool. You can then begin analyzing why the Dublin pool was experiencing so many difficulties.

## Viewing the Failure Distribution Report

You can access the Failure Distribution Report from any of the following reports by clicking either the **Expected failure volume** or the **Unexpected failure volume** metric:

- [Top Failures Report in Skype for Business Server](#)
- [Conference Diagnostic Report in Skype for Business Server](#)
- [Peer-to-Peer Activity Diagnostic Report in Skype for Business Server](#)

From the Failure Distribution Report, you can click any of the following metrics to view the [Failure List Report in Skype for Business Server](#):

- Top diagnostic reasons (sessions)
- Top modalities (sessions)
- Top pools (sessions)
- Top sources (sessions)
- Top components (sessions)

- Top from users (sessions)
- Top to users (sessions)
- Top from user agents (sessions)

## Using the Failure Distribution Report

Depending on your monitor size and screen resolution, it's possible that some of the data shown in the Failure Distribution Report might be truncated when you view it onscreen. This is especially true for metrics such as user agents, which can have very long labels. For example, a user agent with a name like "UCCAPI/4.0.7400.0 OC/4.0.7400.0 (Microsoft Lync 2013)" might only partially appear onscreen:

UCCAPI/4.0.7400.0 OC/4.0.7400.0 (Microsoft Ly...

Fortunately, you can see the entire label simply by holding your mouse over the truncated value.

One interesting metric that you can filter on by using the Failure Distribution Report is Diagnostic ID. If you see the same Diagnostic ID cropping up in other reports you can filter on that ID in the Failure Distribution Report and get a very detailed look at exactly where, and how often, that ID has been reported during a failed session.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Failed Distribution Report enables you to filter on such things as the activity type (peer-to-peer session or conferencing session) or by the diagnostic ID that accompanied each failed session.

The following table lists the filters that you can use with the Failure Distribution Report.

### Failure Distribution Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>Pool</b>	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click <b>[All]</b> to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.
<b>Activity type</b>	Type of activity to filter on. Select one of the following: [All] Peer-to-peer Conference
<b>Session category</b>	Indicates whether the activity in question succeeded or failed. Select one of the following: [All] Success Expected failure Unexpected failure An "expected failure" is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail. An "unexpected failure" is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
<b>Diagnostic ID</b>	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

## Metrics for Top Diagnostic Reasons

The following table lists the information provided in the Failure Distribution Report based on the most frequently reported diagnostic ID.

### Metrics for Top Diagnostic Reasons

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking of failed sessions based on diagnostic IDs. The diagnostic ID is a unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
<b>Top diagnostic reasons</b>	No	Diagnostic ID generated in a session.
<b>Sessions</b>	No	Total number of failed sessions where the specified diagnostic ID was generated.

## Metrics for Top Modalities



The following table lists the information provided in the Failure Distribution Report based on the session modalities that experienced the most failures.

### Metrics for Top Modalities

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking based of failed session based on session type (for example, an audio/video conference or a peer-to-peer file transfer session).
<b>Top modalities</b>	No	Session type.
<b>Sessions</b>	No	Total number of failed sessions involving the specified modality.

### Metrics for Top Pools

The following table lists the information provided in the Failure Distribution Report based on the pools that experienced the most failures.

### Metrics for Top Pools

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking of failed sessions based on the Registrar pool or Edge Server where the session was conducted.
<b>Top pools</b>	No	Name of the Registrar pool or Edge Server.
<b>Sessions</b>	No	Total number of failed sessions per Registrar pool or Edge Server.

### Metrics for Top Sources

The following table lists the information provided in the Failure Distribution Report based on the computers that experienced the most failures.

### Metrics for Top Sources

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking failed sessions per computer.
<b>Top sources</b>	No	Name of the computer involved in the failed session.
<b>Sessions</b>	No	Total number of failed sessions per computer.

### Metrics for Top Components

The following table lists the information provided in the Failure Distribution Report based on the components that experienced the most failures.

### Metrics for Top Components

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking of failed sessions based on component (for example, ExumRouting, GroupChat, or MediationServer).
<b>Top components</b>	No	Name of the component involved in the failed session.
<b>Sessions</b>	No	Total number of failed sessions per component.

### Metrics for Top From Users

The following table lists the information provided in the Failure Distribution Report based on users who experienced the most failures when they tried to call someone else (known as "From" users).

### Metrics for Top From Users

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking of failed sessions based on the user who was invited to join the session.
<b>Top from users</b>	No	SIP address of the user invited to join the session.
<b>Sessions</b>	No	Total number of failed sessions per user.

### Metrics for Top To Users

The following table lists the information provided in the Failure Distribution Report based on the users who experienced the most failures when another user tried to call them (known as "To" users).

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking of failed sessions based on the user who initiated the session.
<b>Top to users</b>	No	SIP address of the user who initiated the session.
<b>Sessions</b>	No	Total number of failed sessions per user.

### Metrics for Top User Agents

The following table lists the information provided in the Failure Distribution Report based on the endpoint software that experienced the most failures.

## Metrics for Top User Agents

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Rank</b>	No	Relative ranking of failed sessions based on the user agent (software) involved in the session. For example: RTCC/4.0.0.0 Inbound Routing/4.0.0.0.
<b>Top user agents</b>	No	Name of the user agent involved in the failed session.
<b>Sessions</b>	No	Total number of failed sessions per user agent.

# Failure List Report in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Failure List Report in Skype for Business Server.

The Failure List report provides information about the individual participants who took part in a failed peer-to-peer or conferencing session. This information includes the URI of the user who experienced the problem, as well as the SIP Response code and Diagnostic ID associated with the failure.

## Accessing the Failure List Report

The Failure List Report is accessed by clicking any of the following metrics on the [Failure Distribution Report in Skype for Business Server](#):

- Top diagnostic reasons (sessions)
- Top modalities (sessions)
- Top pools (sessions)
- Top sources (sessions)
- Top components (sessions)
- Top from users (sessions)
- Top to users (sessions)
- Top from user agents (sessions)

From the Failure List Report you can access the [Peer-to-Peer Session Detail Report in Skype for Business Server](#) by clicking the Session detail metric for a peer-to-peer session. You can also access the Conference Detail Report by clicking the Conference metric for a conference.

## Making the Best Use of the Failure List Report

In the Failure List Report, you can view a description for each Response code or each Diagnostic ID simply by holding your mouse over that value. For example, if you hold your mouse over Diagnostic ID 7025 you'll see the following displayed in a tooltip:

Internal server error creating media for user.

It's important to note that the Failure List Report does not provide a straightforward way to directly retrieve a list of all the users who participated in at least one failed session, nor does it provide a way to determine which users were most-often involved in a failed session. (For one thing, the Failure List Report has no filtering capabilities.) However, if you export the data and then convert it to a comma-separated values file, you can use Windows PowerShell to find the answers to questions like those. For example, suppose you save the data to a .CSV file named C:\Data\Failure\_List.csv. Based on the data saved in that file, this command lists all the users who were involved in at least one failed session:

```
$failures = Import-Csv -Path " C:\Data\Failure_List.csv"  
$failure |Sort-Object "From user" | Select-Object "From user" -Unique
```

That command will return a list similar to this:

```
From user
----
Pilar.Ackerman@litwareinc.com
Henrik.Jensen@litwareinc.com
Gilead.Amosnino@litwareinc.com
David.Ahs@litwareinc.com
Ken.Myer@litwareinc.com
```

These two commands report back the total number of failed sessions that each user was involved in:

```
$failures = Import-Csv -Path "C:\Data\Failure_List.csv"
$failures | Group-Object "From user" | Select-Object Count, Name | Sort-Object -Property Count -Descending
```

That will return data similar to this:

```
Count      Name
-----
20      Pilar.Ackerman@litwareinc.com
20      David.Ahs@litwareinc.com
16      Gilead.Amosnino@litwareinc.com
16      Ken.Myero@litwareinc.com
14      Henrik.Jensen@litwareinc.com
```

## Filters

None. You cannot filter the Failure List Report.

## Metrics

The following table lists the information provided in the Failure List Report for each failed call.

### Failure List Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Reported time</b>	No	Date and time the report was recorded.
<b>Request</b>	No	SIP request type that failed. For example, INVITE or BYE.
<b>Response code</b>	No	SIP response code sent when the conference failed.
<b>Diagnostic ID</b>	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
<b>Join cost time (ms)</b>	No	Amount of time (in milliseconds) required for the user to join the conference.
<b>From user</b>	No	SIP address of the user who initiated the call.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>From user agent</b>	No	Software used by the endpoint of the user who initiated the call.
<b>To user</b>	No	SIP address of the user who was being called.

# Diagnostic Report in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Diagnostic Report in Skype for Business Server.

The Diagnostic Report provides diagnostic and troubleshooting information for a failed session. This information includes both the Diagnostic ID and the Diagnostic header that were reported when the session failed. The Diagnostic ID is a unique identifier (in the form of an ms-diagnostics header) that gets attached to a SIP message, while the Diagnostic header provides an accompanying description for the Diagnostic ID. The report might also contain valuable troubleshooting details that are known by the reporting component. For example:

- The cause code provided by the PSTN gateway that generated the failure. When an outgoing call fails on the PSTN network, an ISDN User Part (ISUP) cause code is automatically generated. For example, a PSTN gateway might send cause code 34 to indicate that no circuit or channel was available for completing the call.
- Peer FQDN, port, and Winsock errors for connectivity failures.
- Names being looked up for DNS resolution failures. DNS resolution takes place any time a client contacts a name server and requests the IP address that corresponds to specified device name.

## Accessing the Diagnostic Report

The Diagnostic Report can be accessed by clicking the Diagnostic Report (Detail) metric on either the [Peer-to-Peer Session Detail Report in Skype for Business Server](#) or the Conference Detail Report.

## Filters

None. You cannot filter the Diagnostic Report.

## Metrics

The following table lists the information provided in the Diagnostic Report for each session.

### Diagnostic Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Report time</b>	No	Date and time that the report was recorded.
<b>Response code</b>	No	SIP response code sent when the session failed.
<b>Request type</b>	No	SIP request type that failed. For example, INVITE, BYE, or SERVICE.
<b>Source</b>	No	Source of the error.
<b>From user URI</b>	No	SIP address of the user who initiated the session.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>From user agent</b>	No	Software used by the endpoint of the user who initiated the session.
<b>Diagnostic ID</b>	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
<b>Content type</b>	No	Type of media content that failed. For example, a common content type is Application/sdp. Session Description Protocol (SDP) is a standard Internet protocol used for session announcements, session invitations, and other forms of multimedia session initiation.
<b>Application</b>	No	Application involved in the error.
<b>To user URI</b>	No	SIP address of the user who was invited to the session.
<b>Conference join times (ms)</b>	No	Amount of time (in milliseconds) it took for the user to join the conference.
<b>Diagnostic header</b>	No	Diagnostic ID description.

A list of diagnostic errors can be found on the [Ms-Diagnostics Header page](#).



# Media Quality Diagnostic Reports in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Media Quality Diagnostic Reports in Skype for Business Server.

The Media Quality Diagnostic Reports provide information about call quality, and diagnostic and troubleshooting information for failed calls.

## In this section

- [Media Quality Summary Report in Skype for Business Server](#) Provides overall quality data for different endpoint types, including Enterprise Voice peer-to-peer calls, Enterprise Voice conference calls, and calls that rely, at least in part, on the public switched telephone network (PSTN).
- [Media Quality Comparison Report in Skype for Business Server](#) Provides a comparison of call quality values for different types of audio calls (for example, calls made over a wireless network vs. calls made across a wired connection).
- [Server Performance Report in Skype for Business Server](#) Lists the servers that have experienced the most problems, based on measurements of such key quality metrics as degradation, packet loss, and jitter.
- [Location Report in Skype for Business Server](#) Provides a list of network locations and a summary of the media quality of the calls that occur at each location. For purposes of this report, locations are based on IP subnets.
- [Device Report in Skype for Business Server](#) Provides a summary of devices that are used for Enterprise Voice calls and it includes the average media quality of the calls by device.
- [Call List Report in Skype for Business Server](#) Provides detailed information about phone calls made or received within your organization.
- [Call Detail Report in Skype for Business Server](#) Provides detailed information about phone calls made from or received within your organization.
- [Server Media Quality Trend Report in Skype for Business Server](#) Provides a way for you to graphically compare up to five servers on Quality of Experience metrics such as call volume, poor call percentage, packet loss, and jitter.
- [The Media Quality Metrics Distribution Report in Skype for Business Server](#) Provides a graph that shows the distribution values for a Quality of Experience metric such as jitter or packet loss.
- [Location Trend Report in Skype for Business Server](#) Provides call quality trend information for network locations.

# Media Quality Summary Report in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Learn about the Media Quality Summary Report in Skype for Business Server.

The Media Quality Summary Report is perhaps your best bet for analyzing call quality in your organization: this report provides detailed Quality of Experience (QoE) call metrics broken down into the following categories:

- UC Peer to Peer Calls (such as a Skype for Business to Skype for Business call)
- UC Conference Sessions
- PSTN Conference Sessions
- PSTN Calls: Media Bypass
- PSTN Calls (Non-Bypass): UC Leg
- PSTN Calls (Non-Bypass): Gateway Leg
- Other Call Types

When you first open the report, you see summary information for each of these categories. Without leaving the report, you can expand each category to look at subcategories such as calls made from Office Communicator 2007 R2 to Skype for Business. In turn, you can then drill down into these subcategories to see details about each call made within that subcategory.

In Skype for Business Server the Media Quality Summary Report further breaks the data down into three call types: audio calls, video calls, and application sharing calls. Each call type has its own section in the report, and its own custom set of call metrics.

The Media Quality Summary Report also allows you to apply filters that enable you to compare the call quality of wired calls vs. wireless calls, internal calls vs. external calls, and VPN calls vs. non-VPN calls.

## Accessing the Media Quality Summary Report

The Media Quality Summary Report is accessed from the Monitoring Reports home page. You can drill down to the [Call List Report in Skype for Business Server](#) by clicking either of the following metrics:

- Call volume
- Poor call percentage

In addition, you can access the Media Quality Metrics Distribution Report by clicking any of the following audio call metrics:

- Round trip (ms)
- Degradation (MOS)
- Packet loss
- Jitter (ms)
- Healer concealed ratio

- Healer stretched ratio
- Healer compressed ratio

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Media Quality Summary Report enables you to filter the returned data by such things as access type (that is, interval access vs. external access) or by wired/wireless network connection. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Media Quality Summary Report.

### Media Quality Summary Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Access type</b>	<p>Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: [All] Internal External</p>
<b>Network type</b>	<p>Indicates the type of network the client was connected to when the call was placed. Select one of the following: [All] Wired Wireless</p>

NAME	DESCRIPTION
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: [All] VPN Non-VPN

## Metrics

The following table lists the information provided in the Media Quality Summary Report.

### Media Quality Summary Report Metrics: Audio Call Summary

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call type/Endpoint type</b>	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: UC Peer-to-Peer Calls UC Conference Sessions PSTN Conference Sessions PSTN Calls: Media Bypass PSTN Calls (Non-Bypass): UC Leg PSTN Calls (Non-Bypass): Gateway Leg Other Call Types
<b>Call volume</b>	No	Total number of calls per call type.
<b>Poor call percentage</b>	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Call volume (wireless call)</b>	No	Total number of calls that used a wireless connection.
<b>Call volume (VPN call)</b>	No	Total number of calls that used a VPN connection.
<b>Call volume (external call)</b>	No	Number of calls that used an external connection (that is, a connection outside the internal network).
<b>Round trip (ms)</b>	No	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing, a routing misconfiguration, or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
------	----------------------------	-------------

<b>Degradation (MOS)</b>	No	<p>Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Skype for Business Server a set of algorithms predict how users would have rated a call. High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.</p>
<b>Packet loss</b>	No	<p>Average rate of RTP packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.</p>
<b>Jitter (ms)</b>	No	<p>Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.</p>

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Healer concealed ratio</b>	No	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
<b>Healer stretched ratio</b>	No	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
<b>Healer compressed ratio</b>	No	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

### Media Quality Summary Report Metrics: Video Call Summary

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call type/Endpoint type</b>	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: UC Peer-to-Peer Calls UC Conference Sessions PSTN Conference Sessions PSTN Calls: Media Bypass PSTN Calls (Non-Bypass): UC Leg PSTN Calls (Non-Bypass): Gateway Leg Other Call Types
<b>Call volume</b>	No	Total number of calls per call type.
<b>Poor call percentage</b>	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Call volume (wireless call)</b>	No	Total number of calls that used a wireless connection.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call volume (VPN call)</b>	No	Total number of calls that used a VPN connection.
<b>Call volume (external call)</b>	No	Number of calls that used an external connection (that is, a connection outside the internal network).
<b>Avg bit-rate (Kbits/s)</b>	No	Average video bit rate (in kilobits per second).
<b>Low bit-rate %</b>	No	Percentage of the call where the bit rate was low.
<b>Outbound packet loss</b>	No	Real-Time Transport Protocol (RTP) packet loss for outbound packets. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
<b>Frozen frame %</b>	No	Percentage of "frozen" frames. In a frozen frame, the video stops advancing while the audio portion of the call continues.
<b>Outbound avg frame rate</b>	No	Average frame rate for outbound transmissions during the call.
<b>Inbound avg frame rate</b>	No	Average frame rate for incoming transmissions during the call.
<b>Inbound low frame rate %</b>	No	Percentage of the call where the bit rate for incoming video was low.
<b>Client health %</b>		Indicates the relative health of the client device during the call.

### Media Quality Summary Report Metrics: Application Sharing Call Summary

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call type/Endpoint type</b>	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: UC Peer-to-Peer Calls UC Conference Sessions PSTN Conference Sessions PSTN Calls: Media Bypass PSTN Calls (Non-Bypass): UC Leg PSTN Calls (Non-Bypass): Gateway Leg Other Call Types

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call volume</b>	No	Total number of calls per call type.
<b>Poor call percentage</b>	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Call volume (wireless call)</b>	No	Total number of calls that used a wireless connection.
<b>Call volume (VPN call)</b>	No	Total number of calls that used a VPN connection.
<b>Call volume (external call)</b>	No	Number of calls that used an external connection (that is, a connection outside the internal network).
<b>Jitter (ms)</b>	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
<b>Avg. relative one way</b>	No	Average relative one-way delay between two media endpoints. This is a single-hop latency measure.
<b>Avg. RDP tile processing latency</b>	No	The average RDP tile processing latency in the AS Conferencing Server over the duration of the viewing session. A high average reflects a longer delay in the viewing experience, and includes network latency. An overloaded conferencing server may experience higher average delays.
<b>Total spoiled tile %</b>	No	Total percentage of spoiled RDP tiles.



# Media Quality Comparison Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Media Quality Comparison Report in Skype for Business Server.

The Media Quality Comparison Report enables you to compare call quality values for different types of audio calls (for example, calls made over a wireless network vs. calls made across a wired connection).

## Accessing the Media Quality Comparison Report

The Media Quality Comparison Report is accessed from the Monitoring Reports home page.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Media Quality Comparison Report.

### Media Quality Comparison Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>Calls</b>	<p>Type of call to be used as the main comparison item. Allowed values are:</p> <ul style="list-style-type: none"> <li>[All]</li> <li>External</li> <li>Internal</li> <li>VPN</li> <li>Non-VPN</li> <li>Wired</li> <li>Wireless</li> <li>External and wired</li> <li>External and wireless</li> <li>External and VPN</li> <li>External and non-VPN</li> <li>Internal and wired</li> <li>Internal and wireless</li> </ul>
<b>Compare with calls</b>	<p>Type of call to be used as the secondary comparison item. Allowed values are:</p> <ul style="list-style-type: none"> <li>[All]</li> <li>External</li> <li>Internal</li> <li>VPN</li> <li>Non-VPN</li> <li>Wired</li> <li>Wireless</li> <li>External and wired</li> <li>External and wireless</li> <li>External and VPN</li> <li>External and non-VPN</li> <li>Internal and wired</li> <li>Internal and wireless</li> </ul>
<b>Interval</b>	<p>Time interval. Select one of the following:</p> <ul style="list-style-type: none"> <li>Hourly (a maximum of 25 hours can be displayed)</li> <li>Daily (a maximum of 31 days can be displayed)</li> <li>Weekly (a maximum of 12 weeks can be displayed)</li> </ul> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2015 and an end date of 2/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>

## Metrics

The following table lists the information provided in the Media Quality Comparison Report.

### Media Quality Comparison Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call volume</b>	No	Total number of calls.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Degradation (MOS)</b>	No	<p>Average amount of MOS (mean opinion score) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0; a value of 0.5 or less represents acceptable degradation. Historically, mean opinion scores were calculated by having users rate the quality of a call on a scale of 1-to-5. Skype for Business Server uses a set of algorithms to predict how users would have rated a call.</p> <p>High degradation values can be caused by congestion; lack of bandwidth; wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.</p>
<b>Poor call percentage</b>	No	<p>The total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).</p>
<b>Round trip (ms)</b>	No	<p>Average amount of (in milliseconds) required for a Real-Time Transport Protocol packet to travel to another endpoint and then back. Round-trip times of 200 milliseconds or less are considered of acceptable quality.</p> <p>High round-trip values can be caused by international call routing; a routing misconfiguration; or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.</p>
<b>Packet loss</b>	No	<p>Average rate of Real-Time Transport Protocol (RTP) packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion; lack of bandwidth; wireless congestion or interference; or an overloaded media server. Packet loss typically results in distorted or lost audio.</p>
<b>Jitter (ms)</b>	No	<p>Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.</p>

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Healer concealed ratio</b>	No	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
<b>Healer stretched ratio</b>	No	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
<b>Healer compressed ratio</b>	No	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

# Server Performance Report in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Learn about the Server Performance Report in Skype for Business Server.

The Server Performance Report provides a list of Skype for Business Server servers that have experienced the highest percentage of poor calls. The report breaks down servers by server type, reporting separate statistics for the following types:

- Mediation Server
- A/V Conferencing Server
- A/V Edge Server
- Gateway (Mediation Server)
- Gateway (Mediation Server bypass)
- Video (including video metrics for A/V Conferencing servers and A/V Edge servers)
- Application Sharing (including application sharing metrics for A/V Conferencing servers and A/V Edge servers)

It's important to note that the ranking shown in this report as relative rankings. For example, suppose your worst-performing server had one poor call among its 1,000 placed calls. That's a more-than-acceptable percentage of .1%. However, if that's the worst-performing server you have (that is, if all your other servers have a poor call percentage even lower than .1%), then that server will still appear on the Server Performance Report.

## Accessing the Server Performance Report

The Server Performance Report is accessed from the Monitoring Reports home page. You can drill down to the [Call List Report in Skype for Business Server](#) by clicking either of the following metrics:

- Call volume
- Poor call percentage

In addition, you can drill down to the Server Media Quality Trend Report by clicking the following metric:

- Trend

## Making the best use of the Server Performance Report

The Server Performance Report provides a number of ways to filter data; for example, you can filter on network type (calls made from a wired connection vs. calls made from a wireless connection) and access type (calls made from inside the firewall vs. calls made from outside the firewall). It's a good idea when viewing the server performance report to make use of these filters. For example, suppose you have a Mediation Server that has a poor call percentage of 3.24%. If you look solely at wireless calls, that same server might have a poor call percentage approaching 20%. That means that the server was having difficulty with wireless calls, a problem that is partially obscured because the server was not having problems with wired calls.

# Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Server Performance Report enables you to do such things as filter the returned data by server type or by network type (that is, wired or wireless). You can also choose how data should be grouped. In this case, data is grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Server Performance Report.

## Server Performance Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Server type</b>	<p>Indicates the type of server whose performance should be reported. Select one of the following: [All] Mediation Server A/V Conferencing Server A/V Edge Server</p>
<b>Top N</b>	<p>Indicates the number of servers (based on their poor call percentage) to be displayed in each category. For example, if you select <b>5</b> then the five poorest-performing servers are displayed. Select one of the following: [All] 5 10</p>
<b>Access type</b>	<p>Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: [All] Internal External</p>
<b>Network type</b>	<p>Indicates the type of network the client was connected to when the call was placed. Select one of the following: [All] Wired Wireless</p>

NAME	DESCRIPTION
<b>VPN</b>	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: [All] VPN Non-VPN

## Metrics

The following table lists the information provided in the Server Performance Report.

### Server Performance Report Metrics: Audio Call Summary

NAME	CAN SORT ON	DESCRIPTION
<b>Server</b>	No	Name/IP address of the server.
<b>Call volume</b>	No	Total number of calls made.
<b>Poor call percentage</b>	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Round trip (ms)</b>	Yes	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing; a routing misconfiguration; or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
<b>Degradation (MOS)</b>	Yes	Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Skype for Business Server, the Monitoring Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.

NAME	CAN SORT ON	DESCRIPTION
<b>Packet loss</b>	Yes	Average rate of real-time transport protocol (RTP) packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
<b>Jitter (ms)</b>	Yes	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
<b>Healer concealed ratio</b>	Yes	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
<b>Healer stretched ratio</b>	Yes	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
<b>Healer compressed ratio</b>	Yes	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

### Server Performance Report Metrics: Video Call Summary

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
------	----------------------------	-------------



NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call type/Endpoint type</b>	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: UC Peer-to-Peer Calls UC Conference Sessions PSTN Conference Sessions PSTN Calls: Media Bypass PSTN Calls (Non-Bypass): UC Leg PSTN Calls (Non-Bypass): Gateway Leg Other Call Types
<b>Call volume</b>	No	Total number of calls per call type.
<b>Poor call percentage</b>	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Call volume (wireless call)</b>	No	Total number of calls that used a wireless connection.
<b>Call volume (VPN call)</b>	No	Total number of calls that used a VPN connection.
<b>Call volume (external call)</b>	No	Number of calls that used an external connection (that is, a connection outside the internal network).
<b>Avg bit-rate (Kbits/s)</b>	No	Average video bit rate (in kilobits per second).
<b>Low bit-rate %</b>	No	Percentage of the call where the bit rate was low.
<b>Outbound packet loss</b>	No	Real-Time Transport Protocol (RTP) packet loss for outbound packets. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion; lack of bandwidth; wireless congestion or interference; or an overloaded media server. Packet loss typically results in distorted or lost audio.
<b>Frozen frame %</b>	No	Percentage of "frozen" frames. In a frozen frame, the video stops advancing while the audio portion of the call continues.
<b>Outbound avg frame rate</b>	No	Average frame rate for outbound transmissions during the call.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Inbound avg frame rate</b>	No	Average frame rate for incoming transmissions during the call.
<b>Inbound low frame rate %</b>	No	Percentage of the call where the bit rate for incoming video was low.
<b>Client health %</b>		Indicates the relative health of the client device during the call.

### Server Performance Report Metrics: Application Sharing Call Summary

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call type/Endpoint type</b>	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: UC Peer-to-Peer Calls UC Conference Sessions PSTN Conference Sessions PSTN Calls: Media Bypass PSTN Calls (Non-Bypass): UC Leg PSTN Calls (Non-Bypass): Gateway Leg Other Call Types
<b>Call volume</b>	No	Total number of calls per call type.
<b>Poor call percentage</b>	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Call volume (wireless call)</b>	No	Total number of calls that used a wireless connection.
<b>Call volume (VPN call)</b>	No	Total number of calls that used a VPN connection.
<b>Call volume (external call)</b>	No	Number of calls that used an external connection (that is, a connection outside the internal network).
<b>Jitter (ms)</b>	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
<b>Avg. relative one way</b>	No	Average relative one-way delay between two media endpoints. This is a single-hop latency measure.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Avg. RDP tile processing latency</b>	No	The average RDP tile processing latency in the AS Conferencing Server over the duration of the viewing session. This metric does not cover network latency. A high average reflects a longer delay in the viewing experience. An overloaded conferencing server may experience higher average delays.
<b>Total spoiled tile %</b>	No	Total percentage of spoiled RDP tiles.

# Location Report in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn about the Location Report in Skype for Business Server.

The Location Report provides information about call quality metrics grouped by network location (that is, by network subnet). If your users are experiencing problems with their calls, this report can help you determine if those problems are widespread or if they are largely confined to a given network segment.

## Accessing the Location Report

The Location Report is accessed from the Monitoring Reports home page. You can drill down to the Call List Report by clicking either of the following metrics:

- Call volume
- Poor call percentage

## Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. For example, the Location Report enables you to filter on such things as the location where a call was originated or whether the call took place on a wireless or a wired connection. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Location Report.

### Location Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Caller location</b>	IP subnet of the user who placed the call. You can only select <b>[All]</b> to indicate all subnets.
<b>Callee location</b>	IP subnet of the user who received the call. You can only select <b>[All]</b> to indicate all subnets.
<b>Network type</b>	<p>Indicates the type of network the client was connected to when the call was placed. Select one of the following:</p> <p>[All] Wired Wireless</p>
<b>VPN</b>	<p>Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following:</p> <p>[All] VPN Non-VPN</p>

## Metrics

The following table lists the information provided in the Location Report.

### Location Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Caller subnet</b>	No	IP subnet of the user who placed the call.
<b>Callee subnet</b>	No	IP subnet of the user who received the call.
<b>Call volume</b>	Yes	Total number of calls placed.
<b>Poor call percentage</b>	Yes	Percentage of calls classified as poor calls. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Round trip (ms)</b>	Yes	<p>Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality.</p> <p>High round-trip values can be caused by international call routing, a routing misconfiguration, or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.</p>
<b>Degradation (MOS)</b>	Yes	<p>Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Skype for Business Server, a set of algorithms predict how users would have rated a call.</p> <p>High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.</p>
<b>Packet loss</b>	Yes	<p>Average rate of RTP packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.</p>
<b>Jitter</b>	Yes	<p>Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.</p>

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Healer concealed ratio</b>	Yes	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
<b>Healer stretched ratio</b>	Yes	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
<b>Healer compressed ratio</b>	Yes	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

# Device Report in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Learn about the Device Report in Skype for Business Server.

The Device Report might be better titled the Microphone and Speakers Report; that's because the Device Report retrieves call-related metrics (such as poor call percentage, echo, and voice switch time) grouped by the microphones and speakers used in the call. If you are interested in IP phones (also commonly referred to as "devices"), use the [IP Phone Inventory Report in Skype for Business Server](#) instead.

The Device Report is extremely useful for administrators in determining if a specific type of device is experiencing high volumes of poor quality calls than others. In turn, this could influence any decisions you must make when it comes time to buy new devices or to replace existing devices.

By default, the information displayed in the Device Report is also based on the microphone (the capture device) and speakers/headset (the render device) used in the call. For example, suppose you have several users who use the following capture device and the following render device: By default, the information displayed in the Device Report is also based on the microphone (the capture device) and speakers/headset (the render device) used in the call. For example, suppose you have several users who use the following capture device and the following render device:

- Capture device -- Microphone (SoundMAX Integrated Digital HD Audio)
- Render device -- Headset Earphone (Microsoft LifeChat LX-3000)

If those users made a total of 254 calls you'll see an entry like this in the report:

CAPTURE DEVICE	RENDER DEVICE	CALL VOLUME
Microphone (SoundMAX Integrated Digital HD Audio)	Headset Earphone (Microsoft LifeChat LX-3000)	254

Now, suppose you have a number of users who use that same capture device but a different render device. In that case, you'll have a second line entry in the report, one for that unique combination of capture device and render device:

CAPTURE DEVICE	RENDER DEVICE	CALL VOLUME
Microphone (SoundMAX Integrated Digital HD Audio)	Headset Earphone (Microsoft LifeChat LX-3000)	254
Microphone (SoundMAX Integrated Digital HD Audio)	Speakers (SoundMAX Integrated Digital HD Audio)	319

If you would rather see combined totals for a given device (for example, for the SoundMAX capture device, regardless of the render device used), select the appropriate option from the Device type dropdown list (either Capture device or Render device). If you select Capture device in this example, that will give you output similar to this:

CAPTURE DEVICE	CALL VOLUME
Microphone (SoundMAX Integrated Digital HD Audio)	573



## Accessing the Device Report

The Device Report is typically accessed from the Monitoring Reports home page. However, if you are viewing the [Call Detail Report in Skype for Business Server](#) you can drill down to the Device Report for a specific device by clicking either of the following metrics:

- Capture Device
- Render Device

From the Device Report you can drill down to the [Call List Report in Skype for Business Server](#) by clicking either of the following metrics:

- Call volume
- Poor call percentage

## Making the Best Use of the Device Report

When it comes to device names, the Device Report is extremely detailed; for example, suppose you have the following capture devices:

- Aastra 3002 Microphone (2- Aastra 3002)
- Aastra 3002 Microphone (3- Aastra 3002)
- Aastra 3002 Microphone (Aastra 3002)
- Aastra 6725ip
- Aastra 6725ip Microphone (10- Aastra 6725ip)
- Aastra 6725ip Microphone (10- Aastra 6725ip)-V0
- Aastra 6725ip Microphone (2- Aastra 6725ip)
- Aastra 6725ip Microphone (3- Aastra 6725ip)
- Aastra 6725ip Microphone (4- Aastra 6725ip)
- Aastra 6725ip Microphone (5- Aastra 6725ip)
- Aastra 6725ip Microphone (6- Aastra 6725ip)
- Aastra 6725ip Microphone (7- Aastra 6725ip)
- Aastra 6725ip Microphone (9- Aastra 6725ip)
- Aastra 6725ip Microphone (9- Aastra 6725ip)-V0
- Aastra 6725ip Microphone (Aastra 6725ip)
- Aastra 6725ip Microphone (Aastra 6725ip)-V0
- Aastra 6725ip Microphone (USB Audio Device)
- Aastra 6725ip Microphone (USB Audio Device)-V0

## NOTE

Keep in mind that capture device names might not be the same if you are running localized versions of Skype for Business Server. A device named Aastra 6725ip Microphone (Aastra 6725ip)-V0 in US English could have a different name in French or Spanish.

Often times you'll want that level of detail; at other times, however, you might only be interested in how many calls use any Aastra microphone, regardless of model number. One way to get information like that is to export the Device Report data to Microsoft Excel and then save that data to a comma-separated values file (for example, C:\Data\Devices\_Report.csv). You can then use a set of commands similar to these to import the .CSV file into Windows PowerShell and report back the total number of calls made using an Aastra capture device:

```
$devices = Import-Csv "C:\Data\Device_Report.csv"
$sum = $devices | Where-Object {$_.Capture device -match "Aastra"}
$sum | foreach-object {[Int]$x = [Int]$x + [Int]$_."call volume"}
$x
```

That will return a single value representing the total number of calls made using an Aastra capture device. For example: 384

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Device Report enables you to filter on such things as call type (that is, was the call a client call), a conference call, or a public switched telephone network (PSTN) call. You can also choose how data should be grouped. In this case, devices are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Device Report.

### Device Report Filters

NAME	DESCRIPTION
<b>From</b>	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.

NAME	DESCRIPTION
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Voice switch cause</b>	<p>Reason why a call had to be placed into half duplex mode in order to prevent echo. In half duplex mode, communication can travel in only one direction at a time, similar to the way users take turns when communicating with a walkie-talkie. Select one of the following: [All] None Bad timestamp Echo DNLP (dynamic nonlinear processor) Low complexity Bad device state Post-AEC echo (acoustic echo cancellation)</p>
<b>Echo cause</b>	<p>Reason why echo above the accepted level was detected in a call. (In telecommunications, echo is a reflection of sound, the same phenomenon you will hear if you yell down to the bottom of a well.) Select one of the following: [All] None Bad timestamp Post-AEC echo (acoustic echo cancellation) ANLP (adaptive nonlinear processor) DNLP (dynamic nonlinear processor) Microphone clipping</p>
<b>Call type</b>	<p>Indicates the type of call that was made. Select one of the following: [All] Client call PSTN call Conference call</p>
<b>Access type</b>	<p>Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: [All] Internal External</p>
<b>Network type</b>	<p>Indicates the type of network the client was connected to when the call was placed. Select one of the following: [All] Wired Wireless</p>
<b>VPN</b>	<p>Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: [All] VPN Non-VPN</p>
<b>Device type</b>	<p>Indicates the type of device. Select one of the following: Capture device Render device Capture/Render device pair</p>

NAME	DESCRIPTION
<b>Device name</b>	<p>Name of the capture or render device. You can enter the complete device name or any portion of the device name. For example, to find the device Microphone (Microsoft LifeCam VX-1000.), you can enter the complete device name as follows:</p> <p>Microphone (Microsoft LifeCam VX-1000.)</p> <p>Or, you can enter just a portion of the name. For example:</p> <p>LifeCam</p> <p>Note that the preceding filter returns any device that contains the string "LifeCam" anywhere in its name.</p>

## Metrics

The following table lists the information provided in the Device Report.

### Device Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Capture device</b>	Yes	Device (for example, a microphone or webcam) used for transmitting audio.
<b>Render device</b>	Yes	Device (for example, a headset or speakers) used for receiving audio.
<b>Call volume</b>	Yes	Total number of calls placed.
<b>Poor call percentage</b>	Yes	Percentage of calls that were classified as "poor." A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
<b>Unique users</b>	Yes	Unique users who used the device. If a user used the device 13 times he or she would count as one unique user, the same as a user who only used the device a single time.
<b>Ratio of voice switch time</b>	Yes	Percentage of the call that had to be conducted in half duplex mode in order to prevent echo. In half duplex mode, communication can travel in only one direction at a time, similar to the way users take turns when communicating with a walkie-talkie.
<b>Ratio of microphone not functioning</b>	Yes	Percentage of the call in which the capture device was not functioning at an acceptable level. A high values suggests that quality issues with the call were primarily due to the capture device not working as expected.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Ratio of speaker not functioning</b>	Yes	Percentage of the call in which the render device was not functioning at an acceptable level. A high values suggests that quality issues with the call were primarily due to the render device not working as expected.
<b>Calls with voice switch (%)</b>	Yes	Percentage of the total calls which had to be placed into half duplex mode. In half duplex mode, communication can travel in only one direction at a time, similar to the way users take turns when communicating with a walkie-talkie.
<b>Echo microphone in (%)</b>	Yes	Percentage of time when echo was detected in the microphone capture stream. Typically, values are low for headsets or handsets, and higher for speaker phones or stand-alone speakers. For devices that support on-board acoustic echo cancellation, high values indicate echo leak. For other devices, this metric should not be used to evaluate device quality.
<b>Echo send (%)</b>	Yes	Percentage of echo transmitted to other users.
<b>Calls with echo (%)</b>	Yes	Percentage of the total calls that had echo exceeding the acceptable level.

# Call List Report in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Call List Report used in Skype for Business Server.

The Call List Report provides Quality of Experience (QoE) metrics for individual calls made and received in your organization. Note that the actual metrics reported will depend on how you access the Call List report. For example, if you open the report from the [Device Report in Skype for Business Server](#), you'll see metrics such as the following, metrics that are also reported on the Device Report:

- Caller's microphone
- Caller's speaker
- Callee's microphone
- Callee's speaker
- Ratio of voice switch time

However, if you open the Call List Report from the [Location Report in Skype for Business Server](#), you won't see any of those metrics; instead, you'll see metrics like these:

- Round trip (ms)
- Degradation (MOS)
- Packet loss
- Jitter (ms)

Those are the metrics reported on the Location Report. However, from the Call List Report you can always click the Detail metric to provide complete QoE information for any call.

## Accessing the Call List Report

The Call List Report can be accessed from any of the following reports:

- The [Location Report in Skype for Business Server](#) (by clicking the Call volume or Poor call percentage metric)
- The [Device Report in Skype for Business Server](#) (by clicking the Call volume or Poor call percentage metric)
- The [Media Quality Summary Report in Skype for Business Server](#) (by clicking the Call volume or Poor call percentage metric)
- The [Server Performance Report in Skype for Business Server](#) (by clicking the Call volume or Poor call percentage metric)

From within the Call List Report you can access the [Call Detail Report in Skype for Business Server](#) by clicking the Detail metric.

## Making the Best Use of the Call List Report

If you can't remember what some of the Call List Report metrics (such as Ratio voice switch time) actually

measure, hold your mouse over the metric label; a tool tip will then appear giving you a brief description of the metric.

## Filters

None. You cannot filter the Call List Report.

## Metrics

The following table lists the information provided in the Call List Report for each call.

### Call List Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Details</b>	No	When you click this item, the report shows additional information on the call.
<b>Caller</b>	Yes	SIP address of the person who initiated the call.
<b>Callee</b>	Yes	SIP address of the person who was called.
<b>Start time</b>	Yes	Date and time that the call started.
<b>End time</b>	Yes	Date and time that the call ended.
<b>Caller user agent</b>	Yes	Software used by the endpoint of the person who initiated the call.
<b>Callee user agent</b>	Yes	Software used by the endpoint of the person who was called.
<b>Round trip (ms)</b>	Yes	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing, a routing misconfiguration, or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Degradation (MOS)</b>	Yes	<p>Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Skype for Business Server, a set of algorithms predict how users would have rated a call.</p> <p>High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.</p>
<b>Packet loss</b>	Yes	<p>Average rate of RTP packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.</p>
<b>Jitter</b>	Yes	<p>Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.</p>
<b>Healer concealed ratio</b>	Yes	<p>Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.</p>
<b>Healer stretched ratio</b>	Yes	<p>Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.</p>



NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Healer compressed ratio</b>	Yes	<p>Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.)</p> <p>High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.</p>
<b>Connectivity</b>	Yes	<p>Type of wireless communication link. Typically, this is one of the following:</p> <ul style="list-style-type: none"> <li>Relay</li> <li>Direct</li> </ul>

# Call Detail Report in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Call Detail Report used in Skype for Business Server.

The Call Detail Report provides a detailed look at an individual call; the report includes nearly all the Quality of Experience metrics and statistics collected by Skype for Business Server, divided into report sections such as:

- Call Information
- Caller Device and Signal Metrics
- Callee Device and Signal metrics
- Caller Client Event
- Callee Client Event
- Audio Stream (Caller to Callee)
- Video Stream (Caller to Callee)
- Audio Stream (Callee to Caller)
- Video Stream (Callee to Caller)

Keep in mind that the categories and the metrics you see on a given report depend on two things: the type of session and the type of endpoints used in the session. For example, an audio-only call will not report metrics for video streams; that's because the call didn't have a video stream. Likewise, you might have a report that lists caller statistics but not callee statistics. That's typically because the callee was not using a SIP-compliant device.

Endpoints are responsible for reporting statistics at the end of a call; however, a cell phone (which knows nothing about SIP or SIP statistics) is unable to report that kind of information. If you call someone and they answer you on their cell phone, you will not get a report from that cell phone when the call ends.

The Call Detail Report is most useful when you are trying to determine exactly why a given call experienced media quality problems.

## Accessing the Call Detail Report

The Call Detail Report can be accessed from any of the following reports:

- The [Location Report in Skype for Business Server \(location-report.md\)](#) (by clicking either the Call volume or the Poor call percentage metric)
- The [Media Quality Summary Report in Skype for Business Server \(summary.md\)](#) (by clicking either the Call volume or Poor call percentage metric)
- The [Media Quality Comparison Report in Skype for Business Server](#) (by clicking the [Call List Report in Skype for Business Server](#) and then clicking the Detail metric).
- The [Server Performance Report in Skype for Business Server](#) (by clicking either the Call volume or Poor call percentage metric)
- The [Call List Report in Skype for Business Server](#) (by clicking the Detail metric)

From within the Call Detail Report you can access the [Device Report in Skype for Business Server](#) by clicking

either of the following metrics:

- Capture device
- Render device

You can also access the Server Media Quality Trend Report by clicking the A/V edge server metric.

## Making the Best Use of the Call Detail Report

The Call Detail Report typically includes over 250 different metrics, including such items as Microphone timestamp drift, Low SNR time, and Near end to echo time. If you can't remember what all of these metrics actually measure, try holding your mouse over the metric label; often-times, a tooltip will appear describing that metric.

If you have problems locating a metric, type part of the metric label in the search box, and then click **Find**. For example, if you can't find the Low SNR time metric, type SNR in the search box, and then click **Find**.

Note that the report only tracks information about a call. The call itself is not recorded.

## Filters

None. You cannot filter the Call Detail Report.

## Metrics

The following table lists the information provided in the Call Detail Report for each call.

### Call Detail Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Caller PAI</b>	No	P-Asserted-Identity of the user who initiated the call. The P-Asserted-Identity is used to convey the proven identity of a user within a trusted network.
<b>Caller URI</b>	No	SIP address of the user who initiated the call.
<b>Caller endpoint</b>	No	Device used to make the call.
<b>Caller user agent</b>	No	Software used on the device that made the call.
<b>Call start</b>	No	Date and time that the call was initially placed.
<b>Mediation Server bypass call</b>	No	Indicates whether the call connected to a PSTN voice gateway or qualified IP-PBX without passing through the Mediation Server.
<b>Caller OS</b>	No	Operating system of the caller's computer.

<b>NAME</b>	<b>CAN YOU SORT ON THIS ITEM?</b>	<b>DESCRIPTION</b>
<b>Caller CPU</b>	No	CPU installed in the computer of the user who initiated the call.
<b>Caller CPU core number</b>	No	Processor number in the computer used by the person who initiated the call.
<b>Caller CPU speed</b>	No	Clock speed of the CPU of the computer used by the person who initiated the call.
<b>Caller CPU virtualization</b>	No	Virtualization (if any) used on the computer used by the person who initiated the call.
<b>Callee PAI</b>	No	P-Asserted-Identity of the user who was invited to join the call. The P-Asserted-Identity is used to convey the proven identity of a user within a trusted network.
<b>Callee URI</b>	No	SIP address of the user who was called.
<b>Callee endpoint</b>	No	Device used to receive the call.
<b>Callee user agent</b>	No	Software used on the device that received the call.
<b>Duration</b>	No	Length of time for the call.
<b>Media bypass warning flag</b>	No	Warning issued when the Mediation Server was bypassed.
<b>Callee OS</b>	No	Operating system of the computer for the user who was called.
<b>Callee CPU</b>	No	CPU installed in the computer of the user who was called.
<b>Callee core number</b>	No	Processor number in the computer used by the person who was called.
<b>Callee CPU speed</b>	No	Clock speed of the CPU of the computer used by the person who was called.
<b>Callee CPU virtualization</b>	No	Virtualization (if any) used on the computer used by the person who was called.

# Server Media Quality Trend Report in Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Learn about the Server Media Quality Trend Report in Skype for Business Server.

The Server Media Quality Trend Report provides a way for you to graphically compare up to five servers on Quality of Experience metrics such as call volume, poor call percentage, packet loss, and jitter. This makes it easier to do such things as identify servers that are performing poorly, identify servers that are underutilized, or identify servers that are being overused.

## Accessing the Server Media Quality Trend Report

The Server Media Quality Trend Report can be accessed from either one of the following report:

- [Server Performance Report in Skype for Business Server](#) (by clicking the Trend metric)
- [Call Detail Report in Skype for Business Server](#) (by clicking the A/V edge server metric. If the caller or callee is a server, you can also reach the Server Quality Media Trend Report by clicking the endpoint name.)

## Making the Best Use of Server Media Quality Trend Report

When you click the Trend metric on the [Server Performance Report in Skype for Business Server](#) for a specific server, the Server Media Quality Trend Report will open. However, you will see only a blank instance of that report; the server you selected on the Server Performance Report will not be displayed onscreen. Instead, you will need to select that server from the Servers dropdown. Note, too that the Servers dropdown includes a Select All option. This option will not work if you have more than 5 servers; the Server Media Quality Trend Report can only display data for a maximum of 5 servers at a time.

On the graphs displayed by the Server Media Quality Trend Report, the points labeled Call Volume and Poor Call Percentage are hotlinks; clicking a point on the graph will open an instance of the [Call List Report in Skype for Business Server](#) showing the total calls (or poor calls) for the specified time period.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Server Media Quality Trend Report.

### Server Media Quality Trend Report Filters

NAME	DESCRIPTION
------	-------------

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>Interval</b>	<p>Time interval. Select one of the following: Hourly (a maximum of 25 hours can be displayed) Daily (a maximum of 31 days can be displayed) Weekly (a maximum of 12 weeks can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 8/7/2015 and an end date of 9/28/2015, data is displayed for the days 8/7/2015 12:00 AM to 9/7/2015 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Server type</b>	<p>Type of server involved in the call. Allowed values are: Mediation Server A/V Conferencing Server A/V Edge Server Gateway (Mediation Server) Gateway (Mediation Server Bypass) AS Conferencing Server</p>
<b>Servers</b>	<p>Name of the server involved in the session; this dropdown list is automatically populated for you based on the value of the Server type filter. You can select up to 5 different servers when compiling a report.</p>
<b>Access type</b>	<p>Indicates whether the participant was logged on to the internal network or from the external network. Allowed values are: [All] Internal External</p>

NAME	DESCRIPTION
<b>Network type</b>	Indicates the type of network the participant was connected to. Allowed values are: [All] Wired Wireless
<b>VPN</b>	Indicates whether an external participant was using a virtual private network (VPN) connection during the session. Allowed values are: [All] VPN Non-VPN

## Metrics

The following table lists the information provided in the Server Media Quality Trend Report.

### Server Media Quality Trend Report Metrics

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Call volume</b>	No	Total number of calls.
<b>Degradation (MOS)</b>	No	Average amount of MOS (mean opinion score) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0; a value of 0.5 or less represents acceptable degradation. Historically, mean opinion scores were calculated by having users rate the quality of a call on a scale of 1-to-5. Skype for Business Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion; lack of bandwidth; wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
<b>Poor call percentage</b>	No	The total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).

NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Round trip (ms)</b>	No	Average amount of time (in milliseconds) required for a Real-Time Transport Protocol packet to travel to one endpoint and then back. Round-trip times of 200 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing; a routing misconfiguration; or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
<b>Packet loss</b>	No	Average rate of Real-Time Transport Protocol (RTP) packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion; lack of bandwidth; wireless congestion or interference; or an overloaded media server. Packet loss typically results in distorted or lost audio.
<b>Jitter (ms)</b>	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
<b>Healer concealed ratio</b>	No	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
<b>Healer stretched ratio</b>	No	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.



NAME	CAN YOU SORT ON THIS ITEM?	DESCRIPTION
<b>Healer compressed ratio</b>	No	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

# The Media Quality Metrics Distribution Report in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn about the Media Quality Metrics Distribution Report in Skype for Business Server.

The Media Quality Metrics Distribution Report enables you to see a graph that shows the distribution values for a Quality of Experience metric such as jitter or packet loss. For example, suppose your users make a total of 10 phone calls; those 10 calls report the following roundtrip times:

CALL NUMBER	ROUND TRIP TIME (MILLISECONDS)
1	50
2	50
3	50
4	50
5	50
6	50
7	50
8	4550
9	50
10	50

The average for those round trip times is 500 milliseconds (5000 divided by 10). Five hundred milliseconds is an extremely large round trip time; as a result, you might believe that you have a serious problem with network congestion. (Long round trip times are typically the result of overloaded networks.)

In reality, of course, 90% of your calls had excellent round trip times; you merely had one bad call that skewed the overall results. If you only look at the average round trip time you might jump to a very wrong conclusion.

The Media Quality Metrics Distribution Report helps you avoid jumping to wrong conclusions by showing you a graphical distribution of a specified metric (such as round trip time). These graphs can help make it clear that you had nine very good calls and one very bad call. Admittedly, you might still want to further investigate that one call; however, the fact that 9 out of the 10 calls were very good suggests that there is no reason to make any drastic changes to your network, at least not at this point in time.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Media Quality Metrics Distribution Report.

## Media Quality Metrics Distribution Report Filters

NAME	DESCRIPTION
<b>From</b>	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.
<b>To</b>	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015 Weeks always run from Sunday through Saturday.
<b>Minimum in x axis</b>	Lowest value to be displayed on the X axis of the graph.
<b>Maximum in x axis</b>	Highest value to be displayed on the X axis of the graph.
<b>Access type</b>	Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: [All] Internal External
<b>VPN</b>	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: [All] VPN Non-VPN
<b>Network type</b>	Indicates the type of network the client was connected to when the call was placed. Select one of the following: [All] Wired Wireless

# Location Trend Report in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn about the Location Trend Report in Skype for Business Server.

The Location Trend Report provides call quality trend information for network locations.

## Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Location Trend Report enables you to filter the returned data by such things as access type (that is, interval access vs. external access) or by wired/wireless network connection. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, or week.

The following table lists the filters that you can use with the Location Trend Report.

### Location Trend Report Filters

NAME	DESCRIPTION
<b>From</b>	<p>Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>
<b>To</b>	<p>End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2015 1:00 PM</p> <p>If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2015</p> <p>To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2015</p> <p>Weeks always run from Sunday through Saturday.</p>

NAME	DESCRIPTION
<b>Interval</b>	<p>Time interval. Select one of the following:</p> <p>Hourly (a maximum of 25 hours can be displayed)</p> <p>Daily (a maximum of 31 days can be displayed)</p> <p>Weekly (a maximum of 12 weeks can be displayed)</p> <p>If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 1/1/2011 and an end date of 2/28/2011, data is displayed for the days 8/1/2011 12:00 AM to 9/1/2011 12:00 AM (that is, a total of 31 days' worth of data).</p>
<b>Access type</b>	<p>Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following:</p> <p>[All]</p> <p>Internal</p> <p>External</p>
<b>Network type</b>	<p>Indicates the type of network the client was connected to when the call was placed. Select one of the following:</p> <p>[All]</p> <p>Wired</p> <p>Wireless</p>
<b>VPN</b>	<p>Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following:</p> <p>[All]</p> <p>VPN</p> <p>Non-VPN</p>

# Rate my Call in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn about the Rate My Call feature in Skype for Business Server.

Rate My Call was a new feature in Skype for Business 2015 and 2016 clients on Windows that provides enterprises a way to get feedback from their end-users.

The Rate My Call window offers a "star" rating system and predefined tokens for audio and video calls. In addition, administrators can enable a custom field to provide feedback.

Collected Rate My Call data is not currently included in any existing monitoring report, but it has a separate monitoring report. Data is collected in SQL tables that can be accessed by running SQL queries.

## Rate my Call Prerequisites

Before the users in your Skype for Business Server deployment can access Rate My Call functionality, the following set of components must be deployed and configured:

- You must have Skype for Business Server installed (version 9160 or higher).
- Have your users install and update to the latest version of Skype for Business and also ask them to use the Skype for Business UI.
- Users must be homed on the Skype for Business Server Front End pool.
- You must have a Skype for Business Server monitoring database deployed and associated to your Skype for Business Server pools.
- We recommend deploying Call Quality Dashboard (CQD).

## Configure Rate my Call

The Rate My Call feature is enabled by default in the Client policy with the following settings:

- Rate My Call Display Percentage - 10%
- Rate My Call Allow Custom User Feedback - disabled

There is no action required to enable the base feature, however but if you want custom feedback you will need to enable it separately. The following Windows PowerShell cmdlet is an example of enabling custom end user feedback and changing the interval from 10% to 80%.

```
Set-CSCClientPolicy -Identity <PolicyIdentity> -RateMyCallDisplayPercentage 80 -  
RateMyCallAllowCustomUserFeedback $true
```

## Accessing Rate My Call Data

Data from users is collected in two tables in the monitoring database.

**[QoeMetrics].[dbo].[CallQualityFeedbackToken]** - this table contains results of token polling by end users.

**[QoeMetrics].[dbo].[CallQualityFeedbackTokenDef]** - this table contains token definitions.

Token definitions are coded as follows:

1	DistortedSpeech
2	ElectronicFeedback
3	BackgroundNoise
4	MuffledSpeech
5	Echo
21	FrozenVideo
22	PixelatedVideo
23	BlurryImage
24	PoorColor
25	DarkVideo
101	Audio_SilentLocal
102	Audio_SilentRemote
103	Audio_Echo
104	Audio_BackgroundNoise
105	Audio_LowSound
106	Audio_Dropped
107	Audio_DistortedSpeech
108	Audio_Interrupted
109	Audio_Other
201	Video_NoLocalVideo
202	Video_NoRemoteVideo
203	Video_LowQuality
204	Video_FrozenVideo
205	Video_StoppedUnexpectedly
206	Video_DarkVideo

207	Video_NoAudioSync
208	Video_Other
301	Pstn_DialPad
401	SS_NoContentLocal
402	SS_NoContentRemote
403	SS_CantPresent
404	SS_LowQuality
405	SS_Freezing
406	SS_StoppedUnexpectedly
407	SS_LargeDelay
408	SS_Other
501	Reliabilty_Join
502	Reliabilty_Invite

**[QoeMetrics].[dbo].[CallQualityFeedback]** This table contains polling results from "Star" voting and customer feedback if enabled.

Data from tables can be called by using a **select \* from [Table.Name]** query or by using Microsoft SQL Server Management Studio.

The following SQL queries can be used:

### **Audio**



```

SELECT
    s.ConferenceDateTime
    ,Caller.URI as Caller
    ,CallerCqf.FeedbackText
    ,CallerCqf.Rating
    ,CallerCqfTokenDef.TokenDescription
    ,CallerCqfToken.TokenValue
FROM [Session] s WITH (NOLOCK)
    INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON
        m.ConferenceDateTime = s.ConferenceDateTime
        AND m.SessionSeq = s.SessionSeq
    INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON -- only look at Audio related feedback
        a.MediaLineLabel = m.MediaLineLabel
        and a.ConferenceDateTime = m.ConferenceDateTime
        and a.SessionSeq = m.SessionSeq
        and a.SenderIsCallerPAI = 1
    INNER JOIN [CallQualityFeedback] AS CallerCqf WITH (NOLOCK) ON
        CallerCqf.ConferenceDateTime = s.ConferenceDateTime
        and
        CallerCqf.SessionSeq = s.SessionSeq
    INNER JOIN [CallQualityFeedbackToken] AS CallerCqfToken WITH (NOLOCK) ON
        CallerCqfToken.ConferenceDateTime = s.ConferenceDateTime
        and
        CallerCqfToken.SessionSeq = s.SessionSeq
        and
        CallerCqfToken.FromURI = CallerCqf.FromURI
    INNER JOIN [CallQualityFeedbackTokenDef] AS CallerCqfTokenDef WITH (NOLOCK) ON
        CallerCqfTokenDef.TokenId = CallerCqfToken.TokenId
        and
        (CallerCqfToken.TokenId < 20 or (CallerCqfToken.TokenId > 100 and CallerCqfToken.TokenId < 200)) --
only look at Audio related feedback
    INNER JOIN [User] AS Caller WITH (NOLOCK) ON
        Caller.UserKey = CallerCqf.FromURI

```

## Video

```

SELECT
    s.ConferenceDateTime
    ,Caller.URI as Caller
    ,CallerCqf.FeedbackText
    ,CallerCqf.Rating
    ,CallerCqfTokenDef.TokenDescription
    ,CallerCqfToken.TokenValue
FROM [Session] s WITH (NOLOCK)
    INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON
        m.ConferenceDateTime = s.ConferenceDateTime
        AND m.SessionSeq = s.SessionSeq
    INNER JOIN [VideoStream] AS v WITH (NOLOCK) ON -- only look at Video related feedback
        v.MediaLineLabel = m.MediaLineLabel
        and v.ConferenceDateTime = m.ConferenceDateTime
        and v.SessionSeq = m.SessionSeq
        and v.SenderIsCallerPAI = 1
    INNER JOIN [CallQualityFeedback] AS CallerCqf WITH (NOLOCK) ON
        CallerCqf.ConferenceDateTime = s.ConferenceDateTime
        and
        CallerCqf.SessionSeq = s.SessionSeq
    INNER JOIN [CallQualityFeedbackToken] AS CallerCqfToken WITH (NOLOCK) ON
        CallerCqfToken.ConferenceDateTime = s.ConferenceDateTime
        and
        CallerCqfToken.SessionSeq = s.SessionSeq
        and
        CallerCqfToken.FromURI = CallerCqf.FromURI
    INNER JOIN [CallQualityFeedbackTokenDef] AS CallerCqfTokenDef WITH (NOLOCK) ON
        CallerCqfTokenDef.TokenId = CallerCqfToken.TokenId
        and
        ((CallerCqfToken.TokenId > 20 and CallerCqfToken.TokenId < 100) or (CallerCqfToken.TokenId > 200 and
CallerCqfToken.TokenId < 300)) -- only look at Video related feedback
    INNER JOIN [User] AS Caller WITH (NOLOCK) ON
        Caller.UserKey = CallerCqf.FromURI

```

## Updating Token Definitions

The latest Skype for Business clients report new problem token IDs (> 100) that may not be present in your [QoeMetrics].[dbo].[CallQualityFeedbackTokenDef] table. To update the database table with the latest token definitions, the below SQL command can be run on the monitoring database using Microsoft SQL Server Management Studio. This command will replace all entries in the [QoeMetrics].[dbo].[CallQualityFeedbackTokenDef] table.

```
DELETE FROM [CallQualityFeedbackTokenDef];
INSERT INTO [CallQualityFeedbackTokenDef] (TokenId, TokenDescription) VALUES
(1, N'DistortedSpeech'),
(2, N'ElectronicFeedback'),
(3, N'BackgroundNoise'),
(4, N'MuffledSpeech'),
(5, N'Echo'),
(21, N'FrozenVideo'),
(22, N'PixelatedVideo'),
(23, N'BlurryImage'),
(24, N'PoorColor'),
(25, N'DarkVideo'),
(101, N'Audio_SilentLocal'),
(102, N'Audio_SilentRemote'),
(103, N'Audio_Echo'),
(104, N'Audio_BackgroundNoise'),
(105, N'Audio_LowSound'),
(106, N'Audio_Dropped'),
(107, N'Audio_DistortedSpeech'),
(108, N'Audio_Interrupted'),
(109, N'Audio_Other'),
(201, N'Video_NoLocalVideo'),
(202, N'Video_NoRemoteVideo'),
(203, N'Video_LowQuality'),
(204, N'Video_FrozenVideo'),
(205, N'Video_StoppedUnexpectedly'),
(206, N'Video_DarkVideo'),
(207, N'Video_NoAudioSync'),
(208, N'Video_Other'),
(301, N'Pstn_DialPad'),
(401, N'SS_NoContentLocal'),
(402, N'SS_NoContentRemote'),
(403, N'SS_CantPresent'),
(404, N'SS_LowQuality'),
(405, N'SS_Freezing'),
(406, N'SS_StoppedUnexpectedly'),
(407, N'SS_LargeDelay'),
(408, N'SS_Other'),
(501, N'Reliabilty_Join'),
(502, N'Reliabilty_Invite');
```

# Plan Call Data Connector

9/30/2019 • 3 minutes to read

## Overview

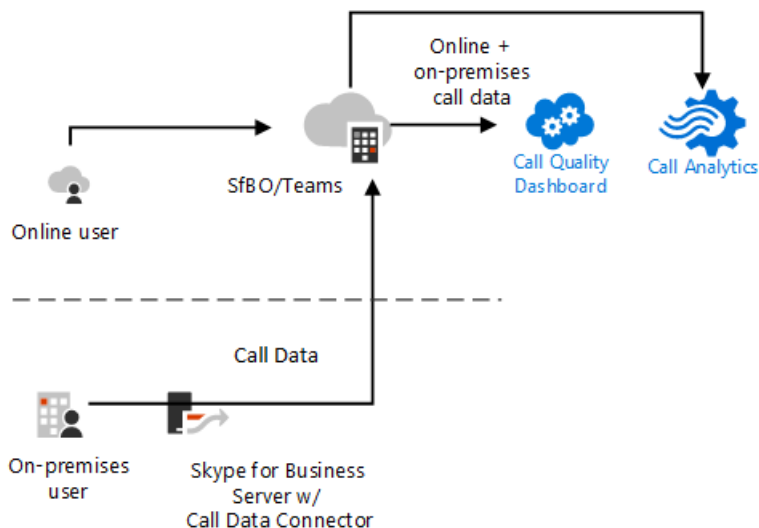
This topic describes benefits, planning considerations, and requirements for implementing Skype for Business Server Call Data Connector. For more information on configuring Call Data Connector, see [Configure Call Data Connector](#).

Call Data Connector greatly simplifies call monitoring in a hybrid environment because you no longer need to use different sets of on-premises and online tools to monitor all of your users call quality. Whether your users are homed on premises or online, you can choose to view call quality for your entire organization online.

With Call Data Connector, you can perform the following tasks by using a single toolset:

- Monitor your user experience across Microsoft Teams, Skype for Business Online, and Skype for Business Server.
- View and troubleshoot problems across your network.
- Assign helpdesk and administrator roles for Call Analytics, so that you can empower helpdesk workers to view and troubleshoot their areas of responsibility.

With Call Data Connector, the Skype for Business Server pushes call data to the cloud service so that you can leverage the Skype for Business Online Call Analytics (CA) and Call Quality Dashboard (CQD) tools, as shown in the following diagram:



The server pushes both Quality of Experience (QoE) and Call Detail Recording (CDR) data to the online service.

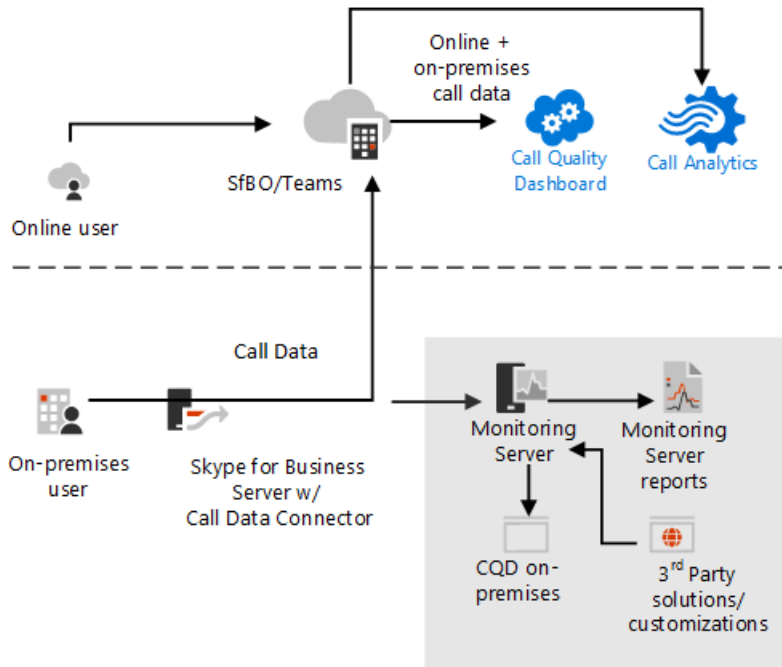
The Call Analytics and CQD tools enable you to monitor the quality of calls and troubleshoot connection problems with Microsoft Teams and Skype for Business services as follows:

- Call Analytics focuses on quality problems with specific calls. It shows detailed information about calls and meetings for each user in a Skype for Business account. With Call Analytics, you can assign permissions to a helpdesk operator who can then monitor calls without having access to the rest of the Skype for Business Admin center.
- Call Quality Dashboard focuses on network performance and issues across an organization. Skype for Business administrators and network engineers use this tool to troubleshoot and optimize network

performance.

For more information, see [Call Analytics and Call Quality Dashboard](#).

Of course, you might want to keep some call quality data on premises. This might be the case, for example, if you are using a third-party solution with customized reports and workflows. Call Data Connector allows you to configure sending data to the online service while also keeping a copy of the data on your on-premises server, as shown in the following diagram:



## Requirements

The following requirements assume that you already have Skype for Business Server deployed in a supported topology. For more information about deploying Skype for Business Server and supported topologies, see [Topology Basics](#). To configure Call Data Connector, you must:

- Enable Hybrid connectivity. If you already have Skype for Business Server deployed and you want to enable Call Data Connector, you must ensure that you have hybrid connectivity set up between your on-premises and online environments. This is sometimes called a split domain configuration.

For more information, see [Plan hybrid connectivity between Skype for Business Server and Office 365](#) and [Configure hybrid connectivity between Skype for Business Server and Office 365](#).

- Authenticate to your Office 365 tenant and ensure that you have the following roles enabled:
  - Skype for Business Server Administrator
  - Office 365 Global Administrator
- If you have not already done so, turn on Call Quality Dashboard as described in [Turning on and using Call Quality Dashboard for Microsoft Teams and Skype for Business Online](#).
- Enable the front end pool for Monitoring, with local LCSCdr and QoEMetrics databases. Without this, Call Data Connector won't have metrics data to work with.

### IMPORTANT

Call Data Connector will not function if Monitoring is not enabled on the front end pool.

- Properly configured [server-to-server authentication](#).

# Comparison of on-premises and online Call Quality Dashboard (CQD) reports

FEATURE REPORTS	SKYPE FOR BUSINESS ONLINE	SKYPE FOR BUSINESS SERVER
Application sharing metric	Yes	Limited
Customer building information	Yes	Yes
Drill-down analytics	Yes	No
Media reliability metrics	Yes	Limited
Out-of-the-box reports	Yes	Yes
Overview reports	Yes	No
Per user reports	Yes	Yes
Report set customization (add, delete, modify reports)	Yes	Yes
Video-based screen sharing metrics	Yes	No
Data APIs for programmatic access to CQD	No	Yes

# Configure Call Data Connector

9/30/2019 • 4 minutes to read

This article describes how to configure Call Data Connector--a single toolset that enables viewing Skype for Business Server Call Quality Data using Skype for Business Online Call Quality Dashboard (CQD) and Call Analytics (CA) tools.

For more information about Call Data Connector benefits and pre-requisites, such as role requirements and setting up hybrid connectivity, see [Plan Call Data Connector](#).

## Enable Monitoring

You must configure Call Data Recording (CDR) and Quality of Experience (QoE) data collection in your front end pool Monitoring, with local LCSCdr and QoEMetrics databases; otherwise, the Call Analytics and Call Quality Dashboards won't get data to work with. Before you Configure Call Data Connector, follow the steps provided in [Deploy monitoring in Skype for Business Server](#) to configure both CDR and QoE as well as basic Monitoring.

### IMPORTANT

Call Data Connector will not function if Monitoring is not enabled on the front end pool.

## Enable Call Data Connector

To configure and enable Call Data Connector, you will use the following cmdlets:

CMDLET	DESCRIPTION
New-CsCloudCallDataConnection	An online cmdlet that establishes an online data collector.
Get-CsCloudCallDataConnection	An online cmdlet that retrieves an existing online data collector.
Get-CsCloudCallDataConnector	An on-premises cmdlet that retrieves the connection information created by the New-CsCloudCallDataConnection cmdlet.
Set-CsCloudCallDataConnector	An on-premises cmdlet that saves an on-premises copy of the connection information created by the New-CsCloudCallDataConnection cmdlet.
Set-CsCloudCallDataConnectorConfiguration	An on-premises cmdlet that allows you to enable or disable the connector and customize the scope level.

### NOTE

To erase your configuration and start over, please use the Remove-csclouddatconnectorconfiguration cmdlet.

### Configure your environment

To configure your environment to enable an online data collector, you must first log in to Skype for Business Online PowerShell as an administrator. For more information, see [Manage Skype for Business Online with Office](#)

## 365 PowerShell.

There are two methods for logging in to Skype for Business Online PowerShell:

- From the Skype for Business Server 2019 management shell (recommended method)
- From another PowerShell session

### Log in to Skype for Business Online PowerShell from the Skype for Business Server management shell (recommended method)

1. If enabling the connector for the first time, run the following command:

```
New-CsCloudCallDataConnection | Set-CsCloudCallDataConnector -TenantId <tenant_id>
```

2. If you get an error that the connection already exists, this means that the call data connection already exists for your tenant. In this case, run the command:

```
Get-CsCloudCallDataConnection | Set-CsCloudCallDataConnector -TenantId <tenant_id>
```

### Log in to Skype for Business Online PowerShell from another PowerShell session (optional method)

1. If enabling the connector for the first time, run the following command:

```
New-CsCloudCallDataConnection
```

2. If you get an error that the connection already exists, this means that the call data connection already exists for your tenant. In this case, run the command:

```
Get-CsCloudCallDataConnection
```

The output of the above commands contains a token value, which you will need when configuring your on-premises environment as follows:

From within the Skype for Business Server management shell, specify the following command:

```
Set-CsCloudCallDataConnector -Identity Global -TenantId <tenant_id> -Token <token-copied-from-online>
```

### Configure the scope

You can enable Call Data Connector for a particular site or for your entire Skype for Business Server deployment by using the `Set-CsCloudCallDataConnectorConfiguration` cmdlet from within the Skype for Business Server management shell. For example, the following command enables Call Data Connector at the global scope:

```
Set-CsCloudCallDataConnectorConfiguration -Identity "global" -EnableCallDataConnector $True
```

In addition to the global settings, Call Data Connector configuration settings can be assigned to the site scope. This provides additional management flexibility when it comes to monitoring. For example, an administrator can enable Call Data Connector forwarding for the Redmond site but disable Call Data Connector forwarding for the Dublin site, as shown in the following example:

```
Set-CsCloudCallDataConnectorConfiguration -Identity "site:Redmond" -EnableCallDataConnector $True
```

```
Set-CsCloudCallDataConnectorConfiguration -Identity "site:Dublin" -EnableCallDataConnector $False
```



Settings configured at the site scope take precedence over settings configured at the global scope. For example, suppose Call Data Connector forwarding is enabled at the global scope, but disabled at the site scope (for the Redmond site). That means that call detail recording and QoE information will not be forwarded for users in the Redmond site. However, users in other sites (that is, users managed by the global settings instead of the Redmond site settings) will have their call detail recording and QoE information forwarded.

Values for the most commonly used settings used by Call Data Connector are shown in the following table:

PROPERTY	DESCRIPTION	DEFAULT VALUE
EnableCallDataConnector	Indicates whether Call Data Connector is enabled. If True, monitoring records will be forwarded to online monitoring.	\$False
Identity	Determines the scope level for the command: global or site.	global

## Disable Call Data Connector

Disabling Call Data Connector does not disassociate the monitoring store from the Front End pool, nor does it uninstall or otherwise affect the backend monitoring database. When you disable Call Data Connector, you stop Skype for Business Server from uploading call data to the cloud.

You disable Call Data Connector by using the `Set-CsCloudCallDataConnectorConfiguration` cmdlet from within the Skype for Business Server management shell. For example, the following command disables Call Data Connector at the global scope by setting the `EnableCallDataConnector` property to `$False`:

```
Set-CsCloudCallDataConnectorConfiguration -Identity "global" -EnableCallDataConnector $False
```

If you want to resume uploading call data to the cloud, set the `EnableCallDataConnector` property back to `$True`, as shown in the following example:

```
Set-CsCloudCallDataConnectorConfiguration -Identity "global" -EnableCallDataConnector $True
```

## View on-premises data through the online dashboard

After Call Data Connector is enabled, you can view your on-premises call data on the Call Analytics dashboard or Call Quality Dashboard as described in [Use Call Analytics to troubleshoot poor quality](#) and [Turn on and use Call Quality Dashboard for Microsoft Teams and Skype for Business Online](#).

## For more information

For more information on the cmdlets, you can use the `Get-Help` command from the Skype for Business Server Management Shell. For example:

`Get-Help Get-CsCloudCallDataConnector | more`

`Get-Help Set-CsCloudCallDataConnector | more`

`Get-Help Set-CsCloudCallDataConnectorConfiguration | more`

# Manage archiving in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn how to manage archiving for Skype for Business Server.

When you deploy archiving for your organization, you specify the initial configuration during deployment. However, there may be times when you want to change how you implement archiving support for day-to-day management or to meet new requirements for your organization. For example, you may need to set up archiving support differently for a specific site, a specific pool, or specific users within your organization. For users homed on Skype for Business Server, you do this by creating and customizing archiving configuration options and user policies.

Before you read this topic, be sure you are familiar with the information in [Plan for archiving in Skype for Business Server](#) and [Deploy archiving for Skype for Business Server](#).

## NOTE

If you enable Microsoft Exchange integration for your deployment, Exchange policies control whether archiving is enabled for the users who are homed on Exchange and have their mailboxes put on In-Place Hold. For details, see [Plan for archiving in Skype for Business Server](#) and [Configure integration with Exchange storage for Skype for Business Server](#).

## Archiving configuration options

Archiving configuration options specify whether to:

- Enable or disable archiving
- Archive IM sessions
- Archive web conferencing sessions
- Block activity when archiving is not available
- Use Exchange integration
- Set up purging and exporting of data

These options can be set at the global, site, or pool level. For more information, see [Manage archiving options in Skype for Business Server](#).

## Archiving policies

Archiving policies determine whether to archive the following:

- Internal communications
- External communications

These policies can be set at the global, site, or user level. For more information, see [Manage archiving policies in Skype for Business Server](#).

## Manage archiving by using the Control Panel or by using Windows PowerShell

You can manage archiving by using the Control Panel or by using Windows PowerShell. The following table summarizes the cmdlets available to help you manage archiving. For details about syntax, including all available parameters, see [Skype for Business Server Management Shell](#).

CMDLET	DESCRIPTION
Export-CsArchivingData	Exports records that have been stored in the Skype for Business Server Archiving database.
Get-CsArchivingConfiguration	Returns information about the archiving configuration settings in your organization.
Get-CsArchivingPolicy	Returns information about your organization's archiving policies for internal and external communications.
Grant-CsArchivingPolicy	Assigns instant messaging (IM) session archiving policies to users or sets of users. These policies give you the ability to archive all IM sessions that take place between internal users, and/or to archive all IM sessions that take place between internal users and external partners.
Invoke-CsArchivingDatabasePurge	Manually purges records from the Archiving database.
New-CsArchivingConfiguration	Creates a new set of instant messaging (IM) settings, which can be used to enable or disable the automatic saving of IM sessions, and to block any instant messages that cannot be archived.
New-CsArchivingPolicy	Creates new instant messaging (IM) session archiving policies. These policies give you the ability to archive all IM sessions that take place between internal users, and/or to archive all IM sessions that take place between internal users and external partners.
Remove-CsArchivingConfiguration	Removes the specified collection of archiving settings that are used to enable or disable the automatic saving of instant messaging (IM) sessions, and to optionally block any instant message that cannot be archived.
Remove-CsArchivingPolicy	Removes the specified instant messaging (IM) archiving policy that determines whether Skype for Business Server will automatically save all IM sessions that take place between internal users, and/or all IM sessions between internal users and federated partners.
Set-CsArchivingConfiguration	Modifies an existing collection of instant messaging (IM) archiving configuration options.
Set-CsArchivingPolicy	Modifies an existing instant messaging (IM) archiving policy. An archiving policy gives you the ability to archive all IM sessions and conferences that take place between internal users; you can also archive sessions that take place between internal users and federated partners.
Set-CsArchivingServer	Enables you to specify a new database location for one or more Archiving Servers.

# Manage archiving options in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to configure archiving options for Skype for Business Server.

You initially configure archiving at deployment, but you can change, add, and delete configurations after deployment. Archiving options determine whether to:

- Enable or disable archiving
- Archive IM sessions
- Archive web conferencing sessions
- Block activity when archiving is not available
- Use Exchange integration
- Set up purging and exporting of data

You can specify configuration options at the following levels:

- Global-level configuration that is created by default when you deploy Skype for Business Server
- Optional site-level configurations that specify how archiving is implemented for a specific site
- Optional pool-level configurations that specify how archiving is implemented for a specific pool

You can delete a site configuration or pool configuration, but you cannot delete the global configuration. If you delete the global configuration, it is automatically reset to the default values. For details about how archiving configurations are implemented and the hierarchy of archiving configurations, see [Plan for archiving in Skype for Business Server](#).

## Configure archiving options by using the Control Panel

You can configure archiving options by using the Control Panel as follows:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Archiving Configuration**.

## Configure archiving options by using Windows PowerShell

You can also configure archiving options by using the Windows PowerShell cmdlets listed in the following table. For details about syntax, including all available parameters, see [Skype for Business Server Management Shell](#).

CMDLET	DESCRIPTION
--------	-------------

<b>CMDLET</b>	<b>DESCRIPTION</b>
Get-CsArchivingConfiguration	Returns information about the archiving configuration settings in your organization.
New-CsArchivingConfiguration	Creates a new set of instant messaging (IM) settings, which can be used to enable or disable the automatic saving of IM sessions, and to block any instant messages that cannot be archived.
Remove-CsArchivingConfiguration	Removes the specified collection of archiving settings that are used to enable or disable the automatic saving of instant messaging (IM) sessions, and to optionally block any instant message that cannot be archived.
Set-CsArchivingConfiguration	Modifies an existing collection of instant messaging (IM) archiving configuration options.

# Create an archiving configuration in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to create an archiving configuration for Skype for Business Server.

## Configure archiving options by using the Control Panel

To configure archiving options for a specific site or pool:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **New**, and then do one of the following:
  - To create a site archiving configuration, click **Site Configuration**, and then in **Select a site**, select the site to be configured for archiving.
  - To create a pool archiving configuration, click **Pool Configuration**, and then in **Select a pool**, select the pool to be configured for archiving.
5. In **New Archiving Setting**, in the **Archiving setting** drop-down list box, do one of the following:
  - To enable archiving only for instant messaging (IM) sessions, click **Archive IM sessions**.
  - To enable archiving for both IM sessions and web conferences, click **Archive IM and web conferencing sessions**.
  - To disable archiving for this configuration, click **Disable archiving**.
6. Also in **New Archiving Setting**, do the following:
  - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
  - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
  - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
    - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
    - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
7. Click **Commit**.

# Configure archiving options by using Windows PowerShell

You can also configure archiving options for a specific site or pool by using the **New-CsArchivingConfiguration** cmdlet.

The following command creates a new collection of archiving configuration settings for the Redmond site:

```
New-CsArchivingConfiguration -Identity "site:Redmond"
```

Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties.

To create settings that use different property values, simply include the appropriate parameter and parameter value. The following example creates a collection of archiving configuration settings that, by default, allow archiving of instant messaging sessions only:

```
New-CsArchivingConfiguration -Identity "site:Redmond" -EnableArchiving "ImOnly"
```

Multiple property values can be modified by including multiple parameters. For example, this command configures the new settings to archive instant messaging sessions and to block instant messaging of the archiving service is not available:

```
New-CsArchivingConfiguration -Identity "site:Redmond" -EnableArchiving "ImOnly" -BlockOnArchiveFailure $True
```

For more information, see the help topic for the [New-CsArchivingConfiguration](#) cmdlet.

# Delete an archiving configuration in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to delete an archiving configuration in Skype for Business Server.

You can delete a site configuration or pool configuration, but you cannot delete the global configuration. If you delete the global configuration, it is automatically reset to the default values.

## Delete an archiving configuration by using the Control Panel

To delete an archiving configuration by using the Control Panel:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. In the list of archiving configurations, click the site or pool configuration that you want to delete, click **Edit**, and then click **Delete**.

### NOTE

You can also click the Global configuration, but choose this option only if you want to reset the Global configuration to the default values.

5. Click **Commit**.

## Delete an archiving configuration by using Windows PowerShell

You can also delete an archiving configuration by using the **Remove-CsArchivingConfiguration** cmdlet.

For example, the following command removes the archiving configuration settings applied to the Redmond site. When a policy configured at the site scope is deleted, users previously managed by the site policy will automatically be governed by the global archiving policy instead:

```
Remove-CsArchivingConfiguration -Identity "site:Redmond"
```

The following command removes all the archiving configuration settings applied to the service scope:

```
Get-CsArchivingConfiguration -Filter "site:*" | Remove-CsArchivingConfiguration
```

The next command removes all the archiving configuration settings where Exchange archiving has been disabled:

```
Get-CsArchivingConfiguration | Where-Object {$_.EnableExchangeArchiving -eq $False} | Remove-CsArchivingConfiguration
```



You can also use the **Remove-CsArchivingConfiguration** cmdlet to reset the global settings to default values. For example, suppose you have enabled IM session archiving at the global level; the following command will reset the value to the default of None, which will disable archiving at the global level:

```
Remove-CsArchivingConfiguration -Identity global
```

For more information, see the help topic for the [Remove-CsArchivingConfiguration](#) cmdlet.

# Enable or disable archiving in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to enable or disable archiving in Skype for Business Server.

## Enable or disable archiving by using the Control Panel

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Select the appropriate global, site, or pool configuration from the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
  - To enable archiving only for instant messaging (IM) sessions, click **Archive IM sessions**.
  - To enable archiving for both IM sessions and conferences, click **Archive IM and conferencing sessions**.
  - To disable archiving for the configuration, click **Disable archiving**.
5. Click **Commit**.

## Enable or disable archiving by using Windows PowerShell

You can also enable or disable archiving by using the **Set-CsArchivingConfiguration** cmdlet. For example, the following command modifies the all of the archiving configuration settings so that only IM sessions are archived. The command calls the **Get-CsArchivingConfiguration** cmdlet without any parameters in order to return all the archiving configuration settings currently in use in the organization. This collection is then piped to the **Where-Object** cmdlet, which selects only those settings where the EnableArchiving property is equal to (-eq) "ImAndWebConf". The filtered collection is then piped to the **Set-CsArchivingConfiguration** cmdlet, which takes each item in the collection and changes the value of EnableArchiving to "ImOnly":

```
Get-CsArchivingConfiguration | Where-Object {$_.EnableArchiving -eq "ImAndWebConf"} | Set-CsArchivingConfiguration -EnableArchiving "ImOnly"
```

# Configure archiving options to handle failures in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to block IM and conferencing sessions in the case of a Skype for Business Server failure that would prevent archiving.

If archiving is a requirement for your organization, you can block IM and conferencing sessions in the event of a Skype for Business Server failure that would prevent archiving. This is sometimes called critical mode. For example, if there is a problem with a storage service, IM would be blocked for users whose communications are enabled for archiving. Both IM and conferencing automatically recover after the failures are corrected.

## Configure critical mode by using the Control Panel

To specify whether communication sessions should be allowed in case of a failure that would prevent archiving:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Click the name of the appropriate global, site, or pool configuration in the list of archiving configurations, click **Edit**, and then click **Show details**.
5. To set how archiving behaves when a failure occurs, select or clear the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
6. Click **Commit**.

## Configure critical mode by using Windows PowerShell

You can also specify whether communication sessions should be allowed in case of a failure that would prevent archiving by using the **Set-CsArchivingConfiguration** cmdlet with the BlockOnArchiveFailure parameter.

For example, the following command disables communications in the case of an archiving failure:

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -BlockOnArchiveFailure $True
```

The next command enables communications in the case of an archiving failure:

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -BlockOnArchiveFailure $False
```

For more information, see the Help topic for the [Set-CsArchivingConfiguration](#) cmdlet.

# Manage purging of archived data in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage purging of archived data for Skype for Business Server.

The Archiving database is not intended for long-term retention, and Skype for Business Server does not provide an e-discovery (search) solution for archived data, so data needs to be moved to other storage. Skype for Business Server provides a session export tool that you can use to export archived data into searchable transcripts. You need to define when to purge archived and exported data.

For more information about exporting data by using the **Export-CsArchivingData** cmdlet, see [Export archived data in Skype for Business Server](#).

## Manage purging of data by using the Control Panel

To manage purging of archived data by using the Control Panel:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Click the name of the appropriate global, site, or pool configuration in the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
  - To enable purging, select the **Enable purging of archiving data** check box and then do one of the following:
    - To purge all records, click the **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
    - To purge only the data that has been exported, click **Purge exported archiving data only**.
  - To disable purging, clear the **Enable purging of archiving data** check box.
5. Click **Commit**.

## Manage purging of data by using Windows PowerShell

You can manage purging of archived data by using the following Windows PowerShell cmdlets:

- **Set-CsArchivingConfiguration** cmdlet with the EnablePurging parameter lets you enable or disable purging of archived data.
- **Invoke-CsArchivingDatabasePurge** lets you manually purge records from the Archiving database.

For example, the following command enables the purging of all archived data. After this command is run, Skype for Business Server will purge all archiving records older than the value specified for the KeepArchivingDataForDays parameter.

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -EnablePurging $True
```

The following command limits purging to archived records that have been exported to a data file (by using the **Export-CsArchivingData** cmdlet). You must also set the `PurgeExportedArchivesOnly` parameter to `True` (`$True`):

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -EnablePurging $True -PurgeExportedArchivesOnly $True
```

After this command is run, Skype for Business Server will only purge archiving records that meet two criteria: 1) they are older than the value specified for the `KeepArchivingDataForDays` parameter; and, 2) they have been exported by using the **Export-CsArchivingData** cmdlet.

To disable the automated purging of archiving records, set the `EnablePurging` parameter to `False` (`$False`):

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -EnablePurging $False
```

The following example uses the **Invoke-CsArchivingDatabasePurge** cmdlet to purge all the records more than 24 hours old from the archiving database on `atl-sql-001.contoso.com`. To ensure that all the records are deleted, including records that have not been exported, the `PurgeExportedArchivesOnly` parameter is set to `False` (`$False`):

```
Invoke-CsArchivingDatabasePurge -Identity "service:ArchivingDatabase:atl-sql-001.contoso.com" -  
PurgeArchivingDataOlderThanHours 24 -PurgeExportedArchivesOnly $False
```

# Manage archiving policies in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage user policies for archiving for Skype for Business Server.

You initially set up archiving policies when you deploy archiving, but you can change, add, and delete configurations after deployment. Archiving policies determine whether to archive:

- Internal communications
- External communications

Archiving policies can be set at the global, site, or user level.

## NOTE

If you enabled Microsoft Exchange integration for your deployment, Exchange policies control whether archiving is enabled for the users who are homed on Exchange and have their mailboxes put on In-Place Hold. For details, see [Plan for archiving in Skype for Business Server](#) and [Configure integration with Exchange storage for Skype for Business Server](#).

## Manage archiving policies by using the Control Panel

You can manage archiving policies by using the Control Panel as follows:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Archiving Policy**

## Manage archiving policies by using Windows PowerShell

You can also configure archiving policies by using the Windows PowerShell cmdlets listed in the following table. For details about syntax, including all available parameters, see [Skype for Business Server Management Shell](#).

CMDLET	DESCRIPTION
Get-CsArchivingPolicy	Returns information about your organization's instant messaging (IM) sessions archiving policies.
Grant-CsArchivingPolicy	Assigns instant messaging (IM) session archiving policies to users or sets of users. These policies give you the ability to archive all IM sessions that take place between internal users, and/or to archive all IM sessions that take place between internal users and external partners.

<b>CMDLET</b>	<b>DESCRIPTION</b>
New-CsArchivingPolicy	Creates new instant messaging (IM) session archiving policies. These policies give you the ability to archive all IM sessions that take place between internal users, and/or to archive all IM sessions that take place between internal users and external partners.
Remove-CsArchivingPolicy	Removes the specified instant messaging (IM) archiving policy that determines whether Skype for Business Server will automatically save all IM sessions that take place between internal users, and/or all IM sessions between internal users and federated partners.
Set-CsArchivingPolicy	Modifies an existing instant messaging (IM) archiving policy. An archiving policy gives you the ability to archive all IM sessions and conferences that take place between internal users; you can also archive sessions that take place between internal users and federated partners.

# Create a new archiving policy in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to create a new archiving policy for Skype for Business Server.

You can create new archiving policies by using the Control Panel or by using Windows PowerShell cmdlets.

## Create a new archiving policy by using the Control Panel

To create a new archiving policy by using the Control Panel:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. Click **New**, and then do one of the following:
  - To create a site-level archiving policy, click **Site policy**, and then, in **Select a site**, click the site to which the policy is to be applied.
  - To create a user-level archiving policy, click **User policy**.
5. In **New Archiving Policy**, do the following:
  - In **Name**, specify a name for the new policy (for example, externalContoso).
  - In **Description**, provide details about what the policy is (for example, External user archiving policy for Contoso).
  - To control archiving of communications with internal users, select or clear the **Archive internal communications** check box.
  - To control archiving of communications with external users, select or clear the **Archive external communications** check box.
6. Click **Commit**.

### IMPORTANT

The settings of a user policy only apply to the specific users and user groups to which you apply the policy. For details, see [Apply an archiving policy to users in Skype for Business Server](#).

## Create a new archiving policy by using Windows PowerShell

You can also create new archiving policies by using the Windows PowerShell **New-CsArchivingPolicy** cmdlet. For more information, see the help topic for the [New-CsArchivingPolicy](#) cmdlet.

### To create a new archiving policy at the site level

This command creates a new archiving policy for the Redmond site:



```
New-CsArchivingPolicy -Identity "site:Redmond"
```

### **To create a new archiving policy at the per-user level**

To create a new archiving policy at the per-user level, simply specify a unique Identity when creating the policy:

```
New-CsArchivingPolicy -Identity "RedmondArchivingPolicy"
```

### **To create a new archiving policy that enables archiving of internal communication sessions**

Because no parameters (other than the mandatory Identity parameter) were specified in the preceding commands, the new policies will use the default values for all their properties. To create policies that use different property values, simply include the appropriate parameter and parameter value. For example, the following command creates an archiving policy that permits archiving of internal instant messaging sessions:

```
New-CsArchivingPolicy -Identity "site:Redmond" -ArchiveInternal $True
```

### **To create a new archiving policy that enables archiving of both internal and external communication sessions**

Multiple property values can be modified by including multiple parameters. For example, this command configures the new policy to archive both internal and external instant messaging sessions:

```
New-CsArchivingPolicy -Identity "site:Redmond" -ArchiveInternal $True -ArchiveExternal $True
```

# Change an existing archiving policy in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to change user archiving policies for Skype for Business Server.

When you first deploy Skype for Business Server, you set up initial archiving policies that determine how archiving is implemented for the users in your deployment. This topic describes how to manage and amend policies.

## Change archiving policies by using the Control Panel

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. In the list of policies, do one of the following:
  - To change the policy for your entire deployment, click **Global** in the list of policies, click **Edit**, and then click **Show details**.
  - To change the policy for a single site, click the site name in the list of policies, click **Edit**, and then click **Show details**.
  - To change the policy for a single user or user group, click the user or user group name in the list of policies, click **Edit**, and then click **Show details**.
5. On the **Edit Archiving Policy** page, do the following:
  - To enable or disable internal archiving for the policy, select or clear the **Archive internal communications** check box.
  - To enable or disable external archiving for the policy, select or clear the **Archive external communications** check box.
6. Click **Commit**.

### IMPORTANT

The settings of a user policy only apply to the specific users and user groups to which you apply the policy. For details, see [Apply an archiving policy to users in Skype for Business Server](#).

## Change archiving policies by using Windows PowerShell

You can also change archiving policies by using the Windows PowerShell **Set-CsArchivingPolicy** cmdlet.

### Enable archiving policies

To enable the archiving of internal communication sessions, set the value of the ArchiveInternal parameter to True (\$True):

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True
```

To enable the archiving of external communication sessions, set the value of the ArchiveExternal parameter to True (\$True):

```
Set-CsArchivingPolicy -Identity "global" -ArchiveExternal $True
```

To enable the archiving of both internal and external communication sessions, set the value of both the ArchiveInternal and ArchiveExternal parameters to True:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True -ArchiveExternal $True
```

### **Disable archiving policies**

To disable archiving altogether, set the value of both the ArchiveInternal and ArchiveExternal parameters to False (\$False):

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $False -ArchiveExternal $False
```

# Apply an archiving policy to users in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to assign an archiving policy to users in Skype for Business Server.

If you have created one or more user policies for archiving for users homed on Skype for Business Server, you can implement archiving support for specific users by applying the appropriate policies to those users or user groups. For example, if you create a policy to support archiving of internal communications, you can apply it to at least one user or user group to support archiving of the user's Skype for Business Server communications.

## NOTE

If you enabled Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange and have their mailboxes put on In-Place Hold. For details, see [Plan for archiving in Skype for Business Server](#) and [Configure integration with Exchange storage for Skype for Business Server](#).

## Apply a user policy by using the Control Panel

To apply a user policy by using the Control Panel:

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**, and then search for the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **Archiving policy**, select the archiving user policy that you want to apply.

## NOTE

The **<Automatic>** settings apply the default server installation settings. These settings are applied automatically by the server.

6. Click **Commit**.

## Apply a user policy by using Windows PowerShell

You can also apply a user policy by using the Windows PowerShell **Grant-CsArchivingPolicy** cmdlet.

The following command assigns the per-user archiving policy RedmondArchivingPolicy to the user Ken Myer.

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName "RedmondArchivingPolicy"
```

This command assigns the per-user archiving policy RedmondArchivingPolicy to all users who have accounts

homed on the Registrar pool atl-cs-001.contoso.com. For details about the Filter parameter used in this command, see the [Get-CsUser](#) cmdlet documentation.

```
Get-CsUser -Filter {RegistrarPool -eq "atl-cs-001.contoso.com"} | Grant-CsArchivingPolicy -PolicyName "RedmondArchivingPolicy"
```

The following command removes any per-user archiving policy previously assigned to Ken Myer. After the per-user policy is removed, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see the [Grant-CsArchivingPolicy](#) cmdlet documentation.

# Delete an existing archiving policy in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to delete an archiving policy for Skype for Business Server.

You can delete a user policy or site policy, but not the global policy. If you delete the global policy, Skype for Business Server automatically resets the policy to the default values.

## Delete a policy by using the Control Panel

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. In the list of archiving policies, click the user or site policy that you want to delete, click **Edit**, and then click **Delete**.
5. Click **Commit**.

## Delete a policy by using Windows PowerShell

You can also delete archiving policies by using the **Remove-CsArchivingPolicy** cmdlet.

For example, the following command deletes the policy with the Identity site:Redmond. When a policy configured at the site level is deleted, users previously managed by the site policy will automatically be governed by the global archiving policy instead:

```
Remove-CsArchivingPolicy -Identity site:Redmond
```

This command removes all the archiving policies applied to the per-user level:

```
Get-CsArchivingPolicy -Filter "tag:*" | Remove-CsArchivingPolicy
```

This command removes all the archiving policies where internal archiving has been disabled:

```
Get-CsArchivingPolicy | Where-Object {$_.ArchiveInternal -eq $False} | Remove-CsArchivingPolicy
```

For more information, see the help topic for the [Remove-CsArchivingPolicy](#) cmdlet.

# Change Archiving database options in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Learn how to change archiving database options for Skype for Business Server.

If you deploy archiving using SQL Server storage for archiving storage for any of your users, you can make the following database storage changes:

- Use a different SQL Server database for archiving storage. This includes the primary Archiving database and any database you use for SQL Server mirroring.
- Switch to Microsoft Exchange integration to store archiving data and files on Exchange servers. If all your users are homed on your Exchange servers and you want to use Microsoft Exchange storage for all users in your deployment, you should remove the SQL Server store databases from your topology.

To make either of these changes, you must run Topology Builder, make the changes, and then publish the topology again. Do not specify **Archiving SQL Server store** or **Enable SQL Server store mirroring** information, unless you have Skype for Business users who are not homed on Exchange servers.

## Change Archiving database options

1. On a computer that is running Skype for Business Server, or on which the Skype for Business Server administrative tools are installed, log on by using an account that is a member of the local Users group (or an account with equivalent user rights).

### NOTE

You can define a topology by using an account that is a member of the local Users group, but to publish a topology, which is required to add a component to the topology, you must use an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (that is, read, write, and modify) on the file share that you are using for the Skype for Business Server file store (that is, so that Topology Builder can configure the required discretionary access control lists (DACLS), or an account with equivalent rights).

2. Start Topology Builder.
3. In the console tree, navigate to the Front End pool in which you deployed Archiving, and then click the name of the Front End pool where you want to change the database options.
4. In the **Action** menu, click **Edit Properties**.
5. In the **Edit Properties** dialog box, click **General**.
6. Scroll down to **Archiving**.
7. In **Archiving**, do the following:
  - To change to a different existing SQL Server store, under **Archiving SQL Server store**, in the drop-down list box, do the following:
  - To use an existing SQL Server store, in the drop-down list box, click the name of the SQL Server store that you want to use.

- To specify a new SQL Server store, click **New**, and then in the **Define New SQL Server store** dialog box, do the following:
  - To use an existing SQL Server store, in the drop-down list box, click the name of the SQL Server store that you want to use.
  - To specify a new SQL Server store, click **New**, and then in the **Define New SQL Server Store** dialog box, do the following:
    - In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server store.
    - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named instance**, and then specify the instance you want to use.
    - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
- To add SQL Server store for mirroring or change to a different existing SQL Server store for SQL Server store mirroring, select **Enable SQL Server store mirroring**, and then do the following:
  - To use an existing SQL Server store for mirroring, in the **Archiving SQL Server store mirror** drop-down list box, click the name of the SQL Server store that you want to use for mirroring.
  - To specify a new SQL Server store for mirroring, click **New**, and then in the **Define New SQL Server Store** dialog box, do one of the following:
    - a. In **SQL Server FQDN**, specify the FQDN of the SQL Server on which you want to create the new SQL Server store.
    - b. Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use.
    - c. If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
- If you enable SQL Server mirroring and want to add or change a SQL Server mirroring witness (a third, separate SQL Server instance that can detect the health of the primary SQL Server server and mirror instances), select the **Use SQL Server mirroring witness to enable automatic failover** check box, and then do one of the following:
  - a. In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server mirroring witness.
  - b. Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use for the mirroring witness.
  - c. If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
- To switch to Microsoft Exchange integration to store archiving data and files on Exchange servers (if all users in your deployment are homed on your Exchange servers), delete all information for Archiving databases.



### IMPORTANT

If you have any Skype for Business users who are not homed on Exchange servers, do not delete the SQL Server store information.

8. To save the configuration, click **OK**.

### IMPORTANT

The changes you make in Topology Builder do not take effect until you publish the new topology. For details, see [Add archiving databases to an existing deployment in Skype for Business Server](#).

## Change the location of the Archiving database by using Windows PowerShell

In most cases, you will not need to change the location of the Archiving database, which is specified when you install Archiving Server. However, if a hardware failure or other problem should occur, you can point Archiving Server to a new database by using the **Set-CsArchivingServer** cmdlet.

The following example changes the location of the Archiving database for the ArchivingServer:atl-cs-001.contoso.com Archiving Server. In this example, the new database is located at ArchivingDatabase:atl-sql-001.contoso.com:

```
Set-CsArchivingServer -Identity "ArchivingServer:atl-cs-001.contoso.com" -ArchivingDatabase  
"ArchivingDatabase:atl-sql-001.contoso.com"
```

# Export archived data in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to export archived data for Skype for Business Server.

Data archived in Archiving databases is not searchable or in a readable format, but you can use the **Export-CsArchivingData** cmdlet to extract records from the database and save them as an Outlook Electronic Mail (EML) file.

If you enable Microsoft Exchange integration, data is archived in Exchange stores. Data archived in Exchange is searchable and discoverable. For details about accessing data that is archived in Exchange, see the Exchange documentation.

## Exporting Archiving Data by Using Windows PowerShell Cmdlets

You can export archived data by using the `Export-CsArchivingData` cmdlet.

The following command exports all the archiving data written to the archiving database `atl-sql-001.contoso.com` since June 1, 2012. The resulting output file will be stored in the folder `C:\ArchivingExports`.

```
Export-CsArchivingData -Identity "ArchivingDatabase:atl-sql-001.contoso.com" -StartDate 6/1/2012 -OutputFolder "C:\ArchivingExports"
```

The following command exports archiving data for a single user: `kenmyer@contoso.com`. This is done by including the `UserUri` parameter followed by the user's SIP address. For example:

```
Export-CsArchivingData -Identity "ArchivingDatabase:atl-sql-001.contoso.com" -StartDate 6/1/2012 -OutputFolder "C:\ArchivingExports" -UserUri "sip:kenmyer@contoso.com"
```

For more information, see the help topic for the [Export-CsArchivingData](#) cmdlet.

# Manage conferencing in Skype for Business Server

5/20/2019 • 10 minutes to read

**Summary:** Learn how to manage conferencing in Skype for Business Server.

This topic describes how to manage conferencing. For more information about how to plan and deploy conferencing, see [Plan for conferencing in Skype for Business Server](#) and [Deploy conferencing in Skype for Business Server](#).

In Skype for Business Server, you manage the details of conferencing by specifying configuration and policy settings as follows. Note that the terms conferencing and meeting are sometimes used interchangeably. But, in general, you can think of a meeting as a specific instance of conferencing.

- **Conferencing policy settings** encompass a wide variety of scheduling and participation options, ranging from whether a meeting can include IP audio and video to the maximum number of people who can attend. You can use conferencing policies to manage security, bandwidth, and legal aspects of meetings.

Note that conferencing policies are applied to the user or site and cannot be applied to a specific meeting. Therefore, the meeting invitation for the conference can be created some weeks in advance, but the restrictive conferencing policy should be applied to the Meeting Organizer's Skype for Business account just before the conference starts.

If a dedicated account is used for the Meeting Organizer role, the conferencing policy can remain assigned to that account. If the Meeting Organizer uses a general Skype for Business account, the policy must be removed after the conference is finished.

- **Meeting configuration settings** dictate the type of meetings that users can create, in addition to controlling how (or even if) anonymous users and dial-in conferencing users can join these meetings. Note that these settings only affect scheduled meetings. Meeting configurations are applied per pool, per site, or globally.
- **Conferencing configuration settings** determine such things as the maximum allowed size for meeting content and handouts; maximum amount of bandwidth for the Application Sharing Conferencing service; storage limits and expiration periods; the URLs for the internal and external downloads of the supported client; pointers to internal and external URLs where users can obtain conferencing help and resources; and the ports used for application sharing, client audio, file transfers, and media traffic.

These settings allow you to manage the actual servers themselves. These settings can only be set by using Skype for Business Server Management Shell.

- **Dial-in access settings** allow you to define information about whether and how users dial in from a phone. You specify some of the dial-in access information, such as access number, from the Control Panel Conferencing tab and some dial-in information--such as dial plan, voice policy, route, and PSTN usage--from the Control Panel Voice Routing tab.
- **PIN policy settings** allow you to name and define the PIN that participants use for dial-in access.

## Manage conferencing by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell

You can manage most conferencing policies and configuration settings by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell. Some configuration settings are available only by using Skype for Business Server Management Shell.

- To manage conferencing policy settings:
  - In Control Panel, select **Conferencing | Conferencing Policy**.
  - In PowerShell, search for the **-CsConferencingPolicy** cmdlets.
- To manage meeting configuration settings:
  - In Control Panel, select **Conferencing | Meeting configuration**.
  - In Skype for Business Server Management Shell, search for the **-CsMeetingConfiguration** cmdlets.
- To manage dial-in access number settings:
  - In Control Panel, select **Conferencing | Dial-in access number**.
  - In Skype for Business Server Management Shell, search for the **-CsDialInConferencing** cmdlets.
- To manage dial-in access information, such as dial plan, voice policy, route, and PSTN usage:
  - In Control Panel, select **Conferencing | Voice routing**.
  - In Skype for Business Server Management Shell, search for the **-CsDialPlan** and **-CsVoice** cmdlets.
- To manage PIN policy settings:
  - In Control Panel, select **Conferencing | PIN policy**.
  - In Skype for Business Server Management Shell, search for the **-CsPinPolicy** cmdlets.
- To manage conferencing configuration settings, you must use the Skype for Business Server Management Shell. Search for **-CsConferencingConfiguration** cmdlets.

## Skype for Business Server Management Shell cmdlets

You can use the following Skype for Business Server Management Shell cmdlets to manage conferencing:

### Conferencing policy settings

CMDLET	DESCRIPTION
<a href="#">Get-CsConferencingPolicy</a>	Returns information about the conferencing policies that have been configured for use in your organization. Conferencing policies determine the features and capabilities that can be used in a conference; this includes everything from whether or not the conference can include IP audio and video to the maximum number of people who can attend a meeting.
<a href="#">Grant-CsConferencingPolicy</a>	Assigns a conferencing policy at the per-user scope.
<a href="#">New-CsConferencingPolicy</a>	Creates a new conferencing policy for use in your organization.
<a href="#">Remove-CsConferencingPolicy</a>	Removes the specified conferencing policy.
<a href="#">Set-CsConferencingPolicy</a>	Modifies an existing conferencing policy.

### Meeting configuration settings

CMDLET	DESCRIPTION
<a href="#">Get-CsMeetingConfiguration</a>	Returns information about the meeting configuration settings currently in use in your organization. Meeting configuration settings help dictate the type of meetings that users can create, and control how (or even if) anonymous users and dial-in conferencing users can join these meetings.
<a href="#">New-CsMeetingConfiguration</a>	Creates a new collection of meeting configuration settings at the site or service scope. Note that these settings only affect scheduled meetings; they do not affect ad-hoc meetings created by clicking the Meet Now option in Skype for Business.
<a href="#">Remove-CsMeetingConfiguration</a>	Deletes an existing collection of meeting configuration settings.
<a href="#">Set-CsMeetingConfiguration</a>	Modifies the meeting configuration settings currently in use in your organization.

### Conferencing configuration settings

CMDLET	DESCRIPTION
<a href="#">Get-CsConferencingConfiguration</a>	Returns information about the conference configuration settings for your organization. Conference settings determine such things as the maximum-allowed size for conference content and handouts, the content grace period (that is, the amount of time content will be stored before being deleted), and the URLs for the internal and external downloads of the supported client.
<a href="#">New-CsConferencingConfiguration</a>	Creates a new collection of conference configuration settings.
<a href="#">Remove-CsConferencingConfiguration</a>	Removes the specified collection of conference configuration settings.
<a href="#">Set-CsConferencingConfiguration</a>	Modifies an existing collection of conferencing configuration settings.

### Dial-in configuration settings

CMDLET	DESCRIPTION
<a href="#">Get-CsConferenceDirectory</a>	Returns information about the conference directories configured for use in your organization. Conference directories are used to help dial-in conferencing users locate conference information.
<a href="#">Get-CsDialInConferencingConfiguration</a>	Retrieves information about how Skype for Business Server responds when users join or leave a dial-in conference.
<a href="#">Get-CsDialInConferencingAccessNumber</a>	Returns information about all the dial-in conferencing access numbers configured for use in your organization.

CMDLET	DESCRIPTION
<a href="#">Get-CsDialInConferencingDtmfConfiguration</a>	Returns the dual-tone multifrequency (DTMF) signaling settings used for dial-in conferencing. DTMF enables users who dial in to a conference to control conference settings (such as muting and unmuting themselves or locking and unlocking the conference) by using the keypad on their telephone.
<a href="#">Get-CsDialInConferencingLanguageList</a>	Returns a list of languages, including regional/minority languages, supported for use with Skype for Business Server dial-in conferences. These languages are used to relay audio messages and instructions to users participating in a conference by using a telephone.
<a href="#">Get-CsDialPlan</a>	Returns information about the dial plans used in your organization.
<a href="#">Grant-CsDialPlan</a>	Assigns a dial plan to one or more users or groups.
<a href="#">Import-CsLegacyConferenceDirectory</a>	Imports conference directories from Microsoft Office Communications Server 2007 R2 to Skype for Business Server. This helps provide interoperability between Skype for Business Server and Office Communications Server 2007 R2.
<a href="#">Move-CsConferenceDirectory</a>	Moves an existing conference directory from one pool to another. Conference directories are used to help dial-in conferencing users locate conference information.
<a href="#">New-CsConferenceDirectory</a>	Creates a new conference directory for use in your organization. Conference directories are used to help dial-in conferencing users locate conference information.
<a href="#">New-CsDialInConferencingAccessNumber</a>	Creates a new dial-in conferencing access number.
<a href="#">New-CsDialInConferencingConfiguration</a>	Creates a new collection of dial-in conferencing configuration settings. These settings determine how Skype for Business Server responds when users join or leave a dial-in conference. In particular, information is returned regarding whether or not participants are required to record their name when joining a conference, and how (or if) the system announces that someone has joined or left the call.
<a href="#">New-CsDialInConferencingDtmfConfiguration</a>	Creates a new collection of dual-tone multifrequency (DTMF) signaling settings used for dial-in conferencing.
<a href="#">New-CsDialPlan</a>	Creates a new dial plan.
<a href="#">Remove-CsConferenceDirectory</a>	Removes an existing conference directory. Conference directories are used to help dial-in conferencing users locate conference information.
<a href="#">Remove-CsDialInConferencingAccessNumber</a>	Removes an existing dial-in conferencing access number.

CMDLET	DESCRIPTION
<a href="#">Remove-CsDialInConferencingConfiguration</a>	Removes one or more collections of dial-in conferencing configuration settings. These settings determine how Skype for Business Server responds when users join or leave a dial-in conference.
<a href="#">Remove-CsDialInConferencingDtmfConfiguration</a>	Removes an existing collection of dual-tone multi-frequency (DTMF) signaling settings used for dial-in conferencing.
<a href="#">Set-CsDialInConferencingAccessNumber</a>	Modifies the property values of an existing dial-in conferencing access number. Dial-in conferencing provides a way for users to use a "regular" telephone, mobile phone or other device on the public switched telephone network (PSTN) to join the audio portion of a conference.
<a href="#">Set-CsDialInConferencingConfiguration</a>	Modifies settings that determine how Skype for Business Server responds when users join or leave a dial-in conference.
<a href="#">Set-CsDialInConferencingDtmfConfiguration</a>	Modifies the dual-tone multifrequency (DTMF) signaling settings used for dial-in conferencing.
<a href="#">Set-CsDialPlan</a>	Modifies an existing dial plan.

### PIN policy settings

CMDLET	DESCRIPTION
<a href="#">Get-CsPinPolicy</a>	Returns information about the client personal identification number (PIN) policies configured for use in your organization. PIN authentication enables users to access Skype for Business Server by providing a PIN instead of a user name and password.
<a href="#">Grant-CsPinPolicy</a>	Assigns a client personal identification number (PIN) policy to a user or group of users.
<a href="#">New-CsPinPolicy</a>	Creates a new client personal identification number (PIN) policy.
<a href="#">Remove-CsPinPolicy</a>	Removes the specified personal identification number (PIN) policy.
<a href="#">Set-CsPinPolicy</a>	Modifies one or more existing client personal identification number (PIN) policies.

### Other conferencing settings

CMDLET	DESCRIPTION
--------	-------------

CMDLET	DESCRIPTION
<a href="#">Disable-CsMeetingRoom</a>	Disables a Skype for Business Server meeting room. A meeting room is a conferencing device designed to address video conferencing and collaboration scenarios in small conference rooms. When you disable a meeting room object you remove all the Skype for Business Server-specific Active Directory attributes assigned to the user account that represents the meeting room. However, the Active Directory user account itself is not deleted.
<a href="#">Enable-CsMeetingRoom</a>	Enables a Skype for Business Server meeting room. To enable a meeting room you must first create an Active Directory user account that will represent that system. Note that, although meeting room objects are based on user accounts, these objects will not show up when you run the Get-CsUser cmdlet.
<a href="#">Get-CsConferenceDisclaimer</a>	Returns information about the conference disclaimer used in your organization. The conference disclaimer is a message that is displayed to users who join the conference by using a hyperlink (for example, users who paste a link to the conference into a browser such as Windows Internet Explorer).
<a href="#">Get-CsMeetingRoom</a>	Returns information about all the Skype for Business Server meeting rooms configured for use in the organization.
<a href="#">Move-CsMeetingRoom</a>	Moves a Skype for Business Server meeting room object from one Registrar pool to another.
<a href="#">Remove-CsConferenceDisclaimer</a>	Clears the text from the header and body of the conference disclaimer used in your organization. The conference disclaimer is a message that is displayed to users who join the conference by using a hyperlink (for example, users who paste a link to the conference into a browser such as Windows Internet Explorer).
<a href="#">Set-CsMeetingRoom</a>	Modifies the property values of an existing Skype for Business Server meeting room.

## Testing settings

CMDLET	DESCRIPTION
<a href="#">Test-CsASConference</a>	Tests the ability of a pair of users to take part in an application sharing conference.
<a href="#">Test-CsAudioConferencingProvider</a>	Tests to see if a user can connect to his or her audio conferencing provider. An audio conferencing provider is a third-party company that provides organizations with conferencing services. Among other things, audio conferencing providers enable users located off site, and not connected to the corporate network or the Internet, to participate in the audio portion of a conference or meeting.
<a href="#">Test-CsAVConference</a>	Tests the ability of a pair of users to take part in an audio/video (A/V) conference.



CMDLET	DESCRIPTION
<a href="#">Test-CsDataConference</a>	<p>Verifies whether or not a pair of users can participate in a Skype for Business Server web conference that includes activities such as sharing or viewing PowerPoint slides, whiteboards, or polls. The cmdlet also verifies that the Skype for Business Server web conferencing service can discover Office Web Apps Server and that a client can upload a PowerPoint file for broadcast by Office Web Apps Server.</p>
<a href="#">Test-CsDialInConferencing</a>	<p>Checks to see if a user can take part in a dial-in conferencing session.</p>
<a href="#">Test-CsDialPlan</a>	<p>Tests a telephone number against a dial plan (formerly known as a location profile) and returns the normalization rule that will be applied to the number as well as the translated number after the normalization rule has been applied.</p>
<a href="#">Test-CsMxConference</a>	<p>Tests the ability of three users to participate in a Skype for Business Server Mobility Service conference. The Mobility Service enables users of mobile phones such as iPhones and Windows Phones to do such things as exchange instant messages and presence information; store and retrieve voice mail internally instead of with their wireless provider; and take advantage of Skype for Business Server capabilities such as Call via Work and dial-out conferencing.</p> <p><b>Note:</b> Clients that use MCX are not supported in Skype for Business Server 2019.</p>
<a href="#">Test-CsUcwaConference</a>	<p>Tests the ability of a pair of users to schedule, join, and then conduct an online conference using the Unified Communications Web API (UCWA).</p>
<a href="#">Debug-CsDataConference</a>	<p>Returns diagnostic information for the data conferencing capabilities included in Skype for Business Server.</p>

# Manage conferencing policies in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage conferencing policies in Skype for Business Server.

This topic describes how to manage conferencing policies. For more information about how to plan and deploy conferencing, see [Plan for conferencing in Skype for Business Server](#) and [Deploy conferencing in Skype for Business Server](#).

Conferencing policies allow you to define a wide variety of scheduling and participation options, ranging from whether a meeting can include IP audio and video to the maximum number of people who can attend. You can use conferencing policies to manage security, bandwidth, and legal aspects of meetings.

You can define conferencing policy on three levels: global scope, site scope, and user scope. Settings apply to a specific user from the narrowest scope to the widest scope. If you assign a policy to a user, those settings take precedence. If you do not assign a user policy, site settings apply. If no user or site policies apply, global policy provides the default settings.

A global policy exists by default, so you cannot create a new global policy. You also cannot delete the existing global policy, but you can change the existing global policy to customize your default settings.

## Manage conferencing policies by using Skype for Business Server Control Panel

To manage conferencing policies by using Skype for Business Server Control Panel:

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Conferencing Policy**.

## Manage conferencing policies by using Skype for Business Server Management Shell

To manage meetings by using Skype for Business Server Management Shell, use the following cmdlets:

### Conferencing policy settings

CMDLET	DESCRIPTION
<a href="#">Get-CsConferencingPolicy</a>	Returns information about the conferencing policies that have been configured for use in your organization.
<a href="#">Grant-CsConferencingPolicy</a>	Assigns a conferencing policy at the per-user scope.
<a href="#">New-CsConferencingPolicy</a>	Creates a new conferencing policy for use in your organization.

<b>CMDLET</b>	<b>DESCRIPTION</b>
Remove-CsConferencingPolicy	Removes the specified conferencing policy.
Set-CsConferencingPolicy	Modifies an existing conferencing policy.

# View conferencing policies in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to view conferencing policies in Skype for Business Server.

You can view conferencing policies by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## View conferencing policies by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Conferencing Policy**.
4. On the **Conferencing Policy** page, double-click the conferencing policy that you would like to view.
5. In **Edit File Filter**, select the **Show Details** check box.

**Edit Conferencing Policy - <policy>** opens displaying the settings for the selected policy.

For details about configuring the settings, see [Create conferencing policies in Skype for Business Server](#).

## View conferencing policies by using Skype for Business Server Management Shell

To view conferencing policies, use the **Get-CsConferencingPolicy** cmdlet:

```
Get-CsConferencingPolicy
```

The cmdlet returns information such as the following:

Identity	: Global
AllowIPAudio	: True
AllowIPVideo	: True
AllowMultiView	: True
Description	:
AllowParticipantControl	: True
AllowAnnotations	: True
DisablePowerPointAnnotations	: False
AllowUserToScheduleMeetingsWithAppSharing	: True
AllowNonEnterpriseVoiceUsersToDialOut	: False
AllowAnonymousUsersToDialOut	: False
AllowAnonymousParticipantsInMeetings	: True
AllowExternalUsersToSaveContent	: True
AllowExternalUserControl	: False
AllowExternalUsersToRecordMeeting	: False
AllowPolls	: True
AllowSharedNotes	: True
EnableDialInConferencing	: True
EnableAppDesktopSharing	: Desktop
AllowConferenceRecording	: False
EnableP2PRecording	: False
EnableFileTransfer	: True
EnableP2PFileTransfer	: True
EnableP2PVideo	: True
AllowLargeMeetings	: False
EnableDataCollaboration	: True
MaxVideoConferenceResolution	: VGA
MaxMeetingSize	: 250
AudioBitRateKb	: 200
VideoBitRateKb	: 50000
AppSharingBitRateKb	: 50000
FileTransferBitRateKb	: 50000
TotalReceiveVideoBitRateKb	: 6000
EnableMultiViewJoin	: True

For more information, including a complete syntax description and list of parameters, see [Get-CsConferencingPolicy](#).

# Create conferencing policies in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Learn how to create conferencing policies in Skype for Business Server.

You can create conferencing policies by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## Create conferencing policies by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Conferencing Policy**.
4. Click **New**, and then do one of the following:
  - To create a user-level policy, click **User policy**. In **New Conferencing Policy**, in **Name**, type a descriptive name for the policy.
  - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the list of sites, click the site that you want, and then click **OK**.

### NOTE

The site name becomes the conferencing policy name; it cannot be changed.

5. In **Description**, type a description for the policy.
6. Under **Organizer policy**, in **Maximum meeting size**, type the maximum number of users that you want to allow at a meeting. By default, the maximum meeting size is 250.
7. To prevent users from inviting anonymous users to meetings, clear the **Allow participants to invite anonymous users** check box. Anonymous users are users who do not have credentials in your organization's Active Directory Domain Services and who, therefore, are not authenticated. By default, users can invite anonymous users to meetings.
8. In **Recording**, do one of the following:
  - To prevent participants from recording meetings, click **None**. This is the default setting.
  - To allow participants to record meetings, click **Enable recording**.
9. To allow external participants to record meetings, select the **Allow federated and anonymous participants to record** check box. The default is to prevent external participants from recording meetings.
10. In **Audio/video**, do one of the following:

- To prevent the use of audio and video, click **None**.
- To allow the use of audio but not video, click **Enable IP audio**.
- To allow the use of audio and video, click **Enable IP audio/video**. This is the default setting.

11. If you chose to allow the use of audio in **Audio/video**, do the following:

- To prevent users from joining the meeting by dialing in, clear the **Enable PSTN dial-in conferencing** check box. By default, users can dial in to meetings by using the public switched telephone network (PSTN).
- If you allow users to dial in to meetings and you want to allow unauthenticated (anonymous) users to join a meeting by using dial out phoning, select the **Allow anonymous participants to dial out** check box. With dial-out phoning, the conference server calls the user, and the user answers the phone to join the meeting. By default, anonymous users cannot join a meeting by using dial-out phoning.

12. If you chose to allow the use of video in **Audio/video**, check **Allow multiple video streams**.

13. In **Data collaboration**, do one of the following:

- To prevent data collaboration, click **None**.
- To allow data collaboration, click **Enable data collaboration**. This is the default setting.

14. If you chose to allow data collaboration in **Data collaboration**, do the following:

- To prevent external downloads, clear the **Allow federated and anonymous participants to download content** check box. By default, external users can download content.
- To prevent file transfers, clear the **Allow participants to transfer files** check box. By default, users can transfer files.
- To prevent the use of annotations, clear the **Enable annotations** check box. To the use of annotations in shared PowerPoint presentations, clear the **Enable PowerPoint annotations**. By default, annotations are allowed.
- To prevent the use of polls, clear the **Enable polls** check box. By default, polls are allowed.

15. In **Application sharing**, do one of the following:

- To prevent the use of application sharing, click **Disable application sharing**.
- To allow the use of application sharing, click **Enable application sharing**. This is the default setting.

16. If you chose to allow application sharing in **Application sharing**, do the following:

- To prevent meeting participants from taking control of application sharing, clear the **Allow participants to take control** check box. By default, participants can take control of application sharing.
- If you chose to allow meeting participants to take control of application sharing, select the **Allow federated and anonymous participants to take control** check box to allow external users to take control of application sharing. By default, external users cannot take control of application sharing.

17. Under **Participant policy**, do one of the following:

- To prevent both application sharing and desktop sharing, click **Disable application and desktop sharing**.
- To allow application sharing but not desktop sharing, click **Enable application sharing**.

- To allow both application sharing and desktop sharing, click **Enable application and desktop sharing**. This is the default setting.
18. To prevent peer-to-peer file transfers, clear the **Enable peer-to-peer file transfer** check box. By default, peer-to-peer file transfers are allowed.
  19. To allow peer-to-peer recording, select the **Enable peer-to-peer recording** check box. By default, peer-to-peer recording is not allowed.
  20. To allow participants to join with multiple video streams, select the **Enable participants to join with multiple video streams** check box. By default, multiple video streams are allowed.
  21. Click **Commit**.

## Create conferencing policies by using Skype for Business Server Management Shell

To create conferencing policies, use the **New-CsConferencingPolicy** cmdlet.

The following example creates a new conferencing policy with the Identity SalesConferencingPolicy. This policy will use all the default values for a conferencing policy except one: MaxMeetingSize. In this example, the maximum size for a meeting will be set to 50 instead of the default value of 250:

```
New-CsConferencingPolicy -Identity SalesConferencingPolicy -MaxMeetingSize 50
```

For more information, including a complete syntax description and list of parameters, see [New-CsConferencingPolicy](#).



# Modify conferencing policies in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to modify conferencing policies in Skype for Business Server.

You can modify conferencing policies by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## Modify conferencing policies by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Conferencing Policy**.
4. In the list of conferencing policies, click the policy that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit Conferencing Policy**, modify any of the policy settings, except for the policy name, which cannot be modified.
6. Click **Commit**.

## Modify conferencing policies by using Skype for Business Server Management Shell

To modify conferencing policies, use the **Set-CsConferencingPolicy** cmdlet.

The following example modifies a property value of the conferencing policy SalesConferencingPolicy. The command sets the value of the AllowConferenceRecording property to False:

```
Set-CsConferencingPolicy -Identity SalesConferencingPolicy -AllowConferenceRecording $False
```

For more information, including complete syntax and a list of parameters, see [Set-CsConferencingPolicy](#).

# Assign conferencing policies in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to assign conferencing policies in Skype for Business Server.

You can assign conferencing policies to users by using Skype for Business Server Management Shell and the **Grant-CsConferencingPolicy** cmdlet.

## Assign conferencing policies by using Skype for Business Server Management Shell

In the following example, the policy SalesConferencingPolicy is assigned to the user with the Identity "Ken Myer":

```
Grant-CsConferencingPolicy -identity "Ken Myer" -PolicyName SalesConferencingPolicy
```

In the next example, the conferencing policy FinanceConferencingPolicy is assigned to all the users who have accounts in the Finance organizational unit. To assign the same policy to all the users in a given organizational unit (OU), the Get-CsUser cmdlet is used to retrieve all the accounts in that OU. After the user accounts have been retrieved, that information is then piped to the Grant-CsConferencingPolicy cmdlet, which assigns the FinanceConferencingPolicy policy to each user in the collection:

```
Get-CsUser -OU "ou=Finance,dc=litwareinc,dc=com" | Grant-CsConferencingPolicy -PolicyName FinanceConferencingPolicy
```

For more information, including complete syntax and a list of parameters, see [Grant-CsConferencingPolicy](#).

# Delete conferencing policies in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to delete conferencing policies in Skype for Business Server.

You can delete conferencing policies by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## Delete conferencing policies by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Conferencing Policy**.
4. In the list of conferencing policies, click the site or user policy that you want to delete, click **Edit**, and then click **Delete**.

## Delete conferencing policies by using Skype for Business Server Management Shell

To delete conferencing policies, use the **Remove-CsConferencingPolicy** cmdlet.

The following command removes the conferencing policy with the Identity RedmondConferencingPolicy:

```
Remove-CsConferencingPolicy -Identity "RedmondConferencingPolicy"
```

The next command deletes any conferencing policies that allow external users to record the conference:

```
Get-CsConferencingPolicy | Where-Object {$_.AllowExternalUsersToRecordMeetings -eq $True} | Remove-CsConferencingPolicy
```

For more information, including complete syntax and a list of parameters, see [Remove-CsConferencingPolicy](#).

# Manage meeting configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage meeting configuration settings in Skype for Business Server.

This topic describes how to manage meeting configuration settings. For more information about how to plan and deploy conferencing, see [Plan for conferencing in Skype for Business Server](#) and [Deploy conferencing in Skype for Business Server](#).

Meeting configuration settings dictate the type of meetings that users can create, in addition to controlling how (or even if) anonymous users and dial-in conferencing users can join these meetings. Note that these settings only affect scheduled meetings; they do not affect ad-hoc meetings created by clicking the Meet Now option in Skype for Business.

Meeting configuration settings define the following:

- Whether users dialing in from the public switched telephone network (PSTN) go to the lobby
- Who can be a presenter
- Whether conference type is assigned by default
- Whether anonymous (unauthenticated) users are admitted by default

You can define characteristics of meetings by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

You can specify meeting settings at the global level (created by default), site level, or pool level. By default, the global settings define the meeting experience. If you create pool-level settings, those settings apply to all meetings hosted by that pool. If you do not create pool-level settings, site-level settings apply, if they exist. If you do not define site-level settings, the global settings apply to all meetings.

## Manage meeting settings by using Skype for Business Server Control Panel

To manage meeting settings by using Skype for Business Server Control Panel:

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Meeting Configuration**.

## Manage meeting settings by using Skype for Business Server Management Shell

To manage meetings by using Skype for Business Server Management Shell, use the following cmdlets:

### Meeting configuration settings

<b>CMDLET</b>	<b>DESCRIPTION</b>
<a href="#">Get-CsMeetingConfiguration</a>	Returns information about the meeting configuration settings currently in use in your organization.
<a href="#">New-CsMeetingConfiguration</a>	Creates a new collection of meeting configuration settings at the site or service scope.
<a href="#">Remove-CsMeetingConfiguration</a>	Deletes an existing collection of meeting configuration settings.
<a href="#">Set-CsMeetingConfiguration</a>	Modifies the meeting configuration settings currently in use in your organization.

# View meeting configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to view meeting configuration settings in Skype for Business Server.

You can view meeting configuration settings by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## View meeting configuration settings by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Meeting Configuration**.
4. On the **Meeting Configuration** page, click the meeting configuration that you would like to view.
5. In **Edit File Filter**, select the **Show Details** check box.

**Edit Meeting Configuration - <policy>** opens displaying the settings for the selected policy.

For details about configuring the settings, see [Create meeting configuration settings in Skype for Business Server](#).

## View meeting configuration settings by using Skype for Business Server Management Shell

To view information about all your meeting configuration settings, use the **Get-CsMeetingConfiguration** cmdlet:

```
Get-CsMeetingConfiguration
```

This command will return information similar to the following:

```
Identity                : Global
PstnCallersBypassLobby  : True
EnableAssignedConferenceType : True
DesignateAsPresenter    : Company
AssignedConferenceTypeByDefault : True
AdmitAnonymousUsersByDefault : True
RequireRoomSystemsAuthorization : False
LogoURL                  :
LegalURL                  :
HelpURL                   :
CustomFooterText         :
AllowConferenceRecording  : True
```

For more information, including a complete list of parameters, see [Get-CsMeetingConfiguration](#).

# Create meeting configuration settings in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn how to create meeting configuration settings in Skype for Business Server.

You can create meeting configuration settings by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## Create meeting configuration settings by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Meeting Configuration**.
4. On the **Meeting Configuration** page, click **New**, and then do one of the following:
  - To create a site-level policy, click **Site configuration**. In the **Select a Site** search field, type all or part of the name of the site for which you want to define meeting join settings. In the resulting list of sites, click the site you want, and then click **OK**.
  - To create a pool-level policy, click **Pool configuration**. In the **Select a Service** search field, type all or part of the name of the pool service for which you want to define meeting join settings. In the resulting list of services, click the pool you want, and then click **OK**.
5. To route participants who dial in from the public switched telephone network (PSTN) through the lobby, clear the **PSTN callers bypass lobby** check box. By default, participants dialing in from the PSTN go directly to the meeting.
6. To configure who can be a presenter in the meeting, in **Designate as presenter**, do one of the following:
  - To not allow anyone other than the organizer to be a presenter, click **None**.
  - To allow only participants who are members of your organization to be a presenter, click **Company**. This is the default setting.
  - To allow any participants to be a presenter, click **Everyone**.
7. To have the organizer select a conference type when scheduling a meeting, clear the **Assigned conference type by default** check box. By default, the conference type is automatically assigned.
8. To prevent anonymous (unauthenticated) users from being automatically admitted, clear the **Admit anonymous users by default** check box. By default, anonymous users are automatically admitted to meetings.
9. To customize the meeting invite that is sent out to participants, do the following. Note that the maximum length for URLs and custom footer text is 1KB. Except for **Help URL**, if you do not specify a value for the customizations, they will not be included in the meeting. If you do not include a custom help URL, the default help URL for Skype for Business will be displayed in the invite.

- To customize the logo that appears in the meeting invite, in **Logo URL**, enter the location of the logo. The logo must be a GIF or JPG image with a size of 188 by 30 pixels.
- To customize the help text that appears in the meeting invite, in **Help URL**, enter the location of the help text.
- To customize the legal text that appears in the meeting invite, in **Legal text URL**, enter the location of the legal text.
- To customize the footer text that appears in the meeting invite, in **Custom footer text**, enter text.

10. Click **Commit**.

## Create meeting configuration settings by using Skype for Business Server Management Shell

To create meeting configuration settings, use the **New-CsMeetingConfiguration** cmdlet.

The following command creates a new set of meeting configuration settings for the Redmond site:

```
New-CsMeetingConfiguration -Identity "site:Redmond"
```

Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new meeting configuration settings will use the default values for all its properties.

To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of meeting configuration settings that, by default, admit everyone to a meeting as a presenter use a command like this:

```
New-CsMeetingConfiguration -Identity "site:Redmond" -DesignateAsPresenter "Everyone"
```

Multiple property values can be set by including multiple parameters. For example, the following command admits everyone to a meeting as a presenter and also forces PSTN users to wait in the lobby until they are formally admitted to the meeting:

```
New-CsMeetingConfiguration -Identity "site:Redmond" -DesignateAsPresenter "Everyone" -PSTNCallersBypassLobby $True
```

For more information, including a complete list of parameters, see [New-CsMeetingConfiguration](#).



# Modify meeting configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to modify meeting configuration settings in Skype for Business Server.

You can modify meeting configuration settings by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## Modify meeting configuration settings by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Meeting Configuration**.
4. In the list of meeting configurations, click the configuration that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit Meeting Configuration**, modify any of the configuration settings, except for the configuration name, which cannot be modified.
6. Click **Commit**.

## Modify meeting configuration settings by using Skype for Business Server Management Shell

To modify meeting configuration settings, use the **Set-CsMeetingConfiguration** cmdlet.

The command shown in the following example modifies the meeting configuration settings assigned to the Redmond site (-Identity site:Redmond). In this case, the value of the DesignateAsPresenter property is set to Everyone:

```
Set-CsMeetingConfiguration -Identity "site:Redmond" -DesignateAsPresenter "Everyone"
```

For more information, including a complete list of parameters, see [Set-CsMeetingConfiguration](#).

# Delete meeting configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to delete meeting configuration settings in Skype for Business Server.

You can delete meeting configuration settings by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

You can delete a site or user configuration, but you cannot delete the global configuration. If you attempt to delete the global configuration, it is automatically reset to the default values.

## Delete meeting configuration settings by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Meeting Configuration**.
4. In the list of meeting configurations, click the site or pool configuration that you want to delete, click **Edit**, and then click **Delete**.

## Delete meeting configuration settings by using Skype for Business Server Management Shell

To delete meeting settings, use the **Remove-CsMeetingConfiguration** cmdlet.

The following command removes the meeting configuration settings applied to the Redmond site:

```
Remove-CsMeetingConfiguration -Identity "site:Redmond"
```

The next command removes all the meeting configuration settings applied to the site scope:

```
Get-CsMeetingConfiguration -Filter "site:*" | Remove-CsMeetingConfiguration
```

For more information, including a complete list of parameters, see [Remove-CsMeetingConfiguration](#).

# Manage conferencing server configuration settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage conferencing server configuration settings in Skype for Business Server.

This topic describes how to manage conferencing configuration settings. For more information about how to plan and deploy conferencing, see [Plan for conferencing in Skype for Business Server](#) and [Deploy conferencing in Skype for Business Server](#).

Conferencing configuration settings determine such things as the maximum allowed size for meeting content and handouts; maximum amount of bandwidth for the Application Sharing Conferencing service; storage limits and expiration periods; the URLs for the internal and external downloads of the supported client; pointers to internal and external URLs where users can obtain conferencing help and resources; and the ports used for application sharing, client audio, file transfers, and media traffic. These settings allow you to manage the actual servers themselves. These settings can be set by using Skype for Business Server Management Shell.

When you install Skype for Business Server, the system provides you with a single collection of conferencing configuration settings (the global collection). If you need to create custom settings for a site or service, you can do so using the **New-CsConferencingConfiguration** cmdlet. Note that new settings can be applied only at the site or service scope; you cannot create a new global collection of conferencing configuration settings, but you can modify the global collection by using the **Set-CsConferencingConfiguration** cmdlet. In addition, no site or service can host more than one collection of settings. If you try to create new settings for the Redmond site and the Redmond site already hosts a collection of conferencing configuration settings, then your command will fail.

## Manage conferencing configuration settings by using Skype for Business Server Management Shell

To manage conferencing configuration settings by using Skype for Business Server Management Shell, use the following cmdlets:

### Conferencing configuration settings

CMDLET	DESCRIPTION
<a href="#">Get-CsConferencingConfiguration</a>	Returns information about the conferencing configuration settings for your organization.
<a href="#">New-CsConferencingConfiguration</a>	Creates a new collection of conferencing configuration settings.
<a href="#">Remove-CsConferencingConfiguration</a>	Removes the specified collection of conferencing configuration settings.
<a href="#">Set-CsConferencingConfiguration</a>	Modifies an existing collection of conferencing configuration settings.

The following command creates a new collection of conferencing configuration settings for the Redmond site (site:Redmond). In this example, one additional parameter is included (Organization) which is used to set the value of the Organization property to Litwareinc:

```
New-CsConferencingConfiguration -Identity site:Redmond -Organization Litwareinc
```

Note that you can have only one such collection per site, so this command would fail if the Redmond site already has a collection of conferencing configuration settings.

The next example defines a new collection of conferencing configuration settings, which are stored in memory initially, and then applied to the Redmond site at a later time.

The first command uses the **New-CsConferencingConfiguration** cmdlet to create a new, in-memory collection of settings stored in the variable \$x. The InMemory parameter specifies that the collection should be created in memory rather than immediately applied to the Redmond site.

After the collection has been created, the second command sets the value of the Organization property to Litwareinc.

Finally, the third command uses the **Set-CsConferencingConfiguration** cmdlet to actually apply the new settings to the Redmond site:

```
$x = New-CsConferencingConfiguration -Identity site:Redmond -InMemory  
$x.Organization = "Litwareinc"  
Set-CsConferencingConfiguration -Instance $x
```

If you do not call the **Set-CsConferencingConfiguration** cmdlet, the new settings will never take effect. Instead, they will disappear as soon as you end your Windows PowerShell session or delete the variable \$x.

# Manage dial-in conferencing in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Learn how to manage dial-in conferencing in Skype for Business Server.

This topic describes how to manage dial-in conferencing. For more information about how to plan and configure dial-in conferencing at deployment, see [Plan for dial-in conferencing in Skype for Business Server](#) and [Configure dial-in conferencing in Skype for Business Server](#).

You can perform the following tasks to manage dial-in conferencing: enable or disable dial-in conferencing, manage access numbers, manage PIN policies for dial in conferencing, manage conference join and leave announcements, modify key mappings for DTMF commands, and welcome users to dial-in conferencing.

For more information about managing dial plans, see [Create or modify a dial plan in Skype for Business Server](#).

For more information about PSTN usage, see [Configure voice policies, PSTN usage records, and voice routes in Skype for Business](#).

## Manage dial-in conferencing by using Skype for Business Server Control Panel

To manage information about dial-in conferencing:

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**.

To manage information about dial plans and PSTN usage:

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Voice routing**.

## Manage dial-in conferencing by using Skype for Business Server Management Shell

To manage dial-in conferencing by using Skype for Business Server Management Shell, use the following cmdlets:

### Dial-in configuration settings

CMDLET	DESCRIPTION
<a href="#">Get-CsConferenceDirectory</a>	Returns information about the conference directories configured for use in your organization. Conference directories are used to help dial-in conferencing users locate conference information.

CMDLET	DESCRIPTION
<a href="#">Get-CsDialInConferencingConfiguration</a>	Retrieves information about how Skype for Business Server responds when users join or leave a dial-in conference.
<a href="#">Get-CsDialInConferencingAccessNumber</a>	Returns information about all the dial-in conferencing access numbers configured for use in your organization.
<a href="#">Get-CsDialInConferencingDtmfConfiguration</a>	Returns the dual-tone multi-frequency (DTMF) signaling settings used for dial-in conferencing. DTMF enables users who dial in to a conference to control conference settings (such as muting and unmuting themselves or locking and unlocking the conference) by using the keypad on their telephone.
<a href="#">Get-CsDialInConferencingLanguageList</a>	Returns a list of languages, including regional/minority languages, supported for use with Skype for Business Server dial-in conferences. These languages are used to relay audio messages and instructions to users participating in a conference by using a telephone.
<a href="#">Get-CsDialPlan</a>	Returns information about the dial plans used in your organization.
<a href="#">Grant-CsDialPlan</a>	Assigns a dial plan to one or more users or groups.
<a href="#">Import-CsLegacyConferenceDirectory</a>	Imports conference directories from Microsoft Office Communications Server 2007 R2 to Skype for Business Server. This helps provide interoperability between Skype for Business Server and Office Communications Server 2007 R2.
<a href="#">Move-CsConferenceDirectory</a>	Moves an existing conference directory from one pool to another.
<a href="#">New-CsConferenceDirectory</a>	Creates a new conference directory for use in your organization.
<a href="#">New-CsDialInConferencingAccessNumber</a>	Creates a new dial-in conferencing access number.
<a href="#">New-CsDialInConferencingConfiguration</a>	Creates a new collection of dial-in conferencing configuration settings. These settings determine how Skype for Business Server responds when users join or leave a dial-in conference. In particular, information is returned regarding whether or not participants are required to record their name when joining a conference, and how (or if) the system announces that someone has joined or left the call.
<a href="#">New-CsDialInConferencingDtmfConfiguration</a>	Creates a new collection of dual-tone multi-frequency (DTMF) signaling settings used for dial-in conferencing.
<a href="#">New-CsDialPlan</a>	Creates a new dial plan.
<a href="#">Remove-CsConferenceDirectory</a>	Removes an existing conference directory.
<a href="#">Remove-CsDialInConferencingAccessNumber</a>	Removes an existing dial-in conferencing access number.

CMDLET	DESCRIPTION
Remove-CsDialInConferencingConfiguration	Removes one or more collections of dial-in conferencing configuration settings. These settings determine how Skype for Business Server responds when users join or leave a dial-in conference.
Remove-CsDialInConferencingDtmfConfiguration	Removes an existing collection of dual-tone multi-frequency (DTMF) signaling settings used for dial-in conferencing.
Set-CsDialInConferencingAccessNumber	Modifies the property values of an existing dial-in conferencing access number.
Set-CsDialInConferencingConfiguration	Modifies settings that determine how Skype for Business Server responds when users join or leave a dial-in conference.
Set-CsDialInConferencingDtmfConfiguration	Modifies the dual-tone multifrequency (DTMF) signaling settings used for dial-in conferencing.
Set-CsDialPlan	Modifies an existing dial plan.

### PIN policy settings

CMDLET	DESCRIPTION
Get-CsPinPolicy	Returns information about the client personal identification number (PIN) policies configured for use in your organization. PIN authentication enables users to access Skype for Business Server by providing a PIN instead of a user name and password.
Grant-CsPinPolicy	Assigns a client personal identification number (PIN) policy to a user or group of users.
New-CsPinPolicy	Creates a new client personal identification number (PIN) policy.
Remove-CsPinPolicy	Removes the specified personal identification number (PIN) policy.
Set-CsPinPolicy	Modifies one or more existing client personal identification number (PIN) policies.

# Enable or disable dial-in conferencing in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to use Control Panel or Management Shell to enable or disable dial-in conferencing in Skype for Business Server.

You can enable dial-in conferencing by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

## Enable or disable dial-in conferencing by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Conferencing Policy**.
4. In the list of conferencing policies, select the policy for which you want to enable dial-in conferencing, click **Edit**, and then click **Show details**.
5. To allow users to join meeting by dialing in, check the **Enable PSTN dial-in conferencing** check box. By default, users can dial in to meetings by using the public switched telephone network (PSTN).
6. Click **Commit**.

## Enable or disable dial-in conferencing by using Skype for Business Server Management Shell

To enable or disable dial-in conferencing, use the **Set-CsConferencingPolicy** cmdlet with the EnableDialInConferencing parameter as follows:

```
Set-CsConferencingPolicy [-EnableDialInConferencing <$true | $false>]
```

For more information, see [Set-CsConferencingPolicy](#).



# Manage dial-in conferencing access numbers in Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Learn how to manage dial-in conferencing access numbers in Skype for Business Server.

When you deploy dial-in conferencing, you need to set up phone numbers that users can dial from the public switched telephone network (PSTN) to join the audio portion of conferences. These dial-in access numbers appear in meeting invitations and on the Dial-in Conferencing Settings webpage.

This topic describes how to view, modify, or delete existing dial-in conferencing access numbers. For more information about how to create initial dial-in access numbers, see [Configure dial-in conferencing in Skype for Business Server](#).

## View dial-in conferencing access numbers

You can view dial-in conferencing access numbers by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### View dial-in access numbers by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Dial-in Access Number**.
4. On the **Dial-in Access Number** page, click the access number that you would like to view.
5. In **Edit**, select the **Show Details** check box.

### View dial-in access numbers by using Skype for Business Server Management Shell

To view information about dial-in access numbers, use the **Get-CsDialInConferencingAccessNumber** cmdlet.

The following command returns a collection of all the dial-in conferencing access numbers configured for use in the organization:

```
Get-CsDialInConferencingAccessNumber
```

The following is an example of the type of information returned:

```
Identity           : CN={20ca8dc8-5ff8-41f4-b5bb-22ba9972ae2e},
                   : CN=Application Contacts,CN=RTCService=Services,
                   : CN=Configuration,DC=litwareinc,DC=com
PrimaryUri         : sip:testnumber@litwareinc.com
DisplayName        : Test
DisplayNumber      : 1-425-555-1019
LineUri            : tel:+14255551019
PrimaryLanguage    : en-US
SecondaryLanguages : {}
Pool               : atl-cs-001.litwareinc.com
HostingProvider    :
Regions            : {US}
```

For more information, see [Get-CsDialInConferencingAccessNumber](#).

## Modify dial-in conferencing access numbers

You can modify dial-in access numbers by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### Modify dial-in access numbers by using Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Dial-in Access Number**.
4. On the **Dial-in Access Number** page, click one of the dial-in access numbers in the list, click **Edit**, and then click **Show details**.

#### NOTE

Using the search field to search for the contents of a column in the list of dial-in access numbers may not yield the results you expect. Instead, sort the list by the column of interest to identify the dial-in access number you want to view or change.

5. In **Display number**, type the phone number that public switched telephone network (PSTN) phone users dial to join a conference.

This number is displayed in meeting invitations and on the Dial-in Conferencing Settings webpage.

6. In **Display name**, type a description for the dial-in access number. This is the name that is associated with the dial-in access number in Skype for Business search results.

This name is displayed in the client when a user calls the access number.

7. In **Line URI**, type the E.164 number of the dial-in access number in TEL URI format, including the + symbol before the number and excluding spaces. For example, tel:+14255550200.

#### NOTE

The same Line URI cannot be reused by another dial-in conferencing access number.

8. In **SIP URI**, do the following:

In the text box, type a unique SIP URI for this dial-in conferencing access number. This SIP URI is displayed

in various locations including, but not limited to, call notification messages and previous versions of Lync clients.

#### NOTE

The same SIP URI cannot be reused by another dial-in conferencing access number. The SIP URI cannot be modified after the access number is created. The only way to change the SIP URI is to delete and recreate the access number.

In the drop-down list box, click the domain of the Conferencing Attendant application that supports this dial-in access number.

9. In **Pool**, click the pool that is running the instance of Conferencing Attendant that supports this dial-in access number.

#### NOTE

If you need to change the pool after you create the access number, you must use the **Move-CsApplicationEndpoint** cmdlet or delete and recreate the access number.

10. In **Primary language**, click the language in which prompts are played for this dial-in access number.

The primary language is the language that the Conferencing Attendant uses to answer the call. Supported languages are displayed alongside each access phone number on the Dial-in Conferencing Settings webpage.

11. (Optional) In **Secondary languages (maximum of four)**, click **Add**, select one or more additional languages that you want to support for callers to this dial-in access number, and then click **OK**.

You can choose up to four secondary languages for each dial-in access number. Users can select a secondary language before entering the conference ID when they dial in to a conference.

12. To add a region for the dial-in access number, under **Associated regions**, click **Add**, click one or more regions that are associated with the dial plans for this dial-in access number, and then click **OK**.
13. To delete a region from the dial-in access number, under **Associated regions**, click the region you want to delete, and then click **Remove**.
14. Click **Commit**.

### Modify dial-in access numbers by using Skype for Business Server Management Shell

To modify dial-in access numbers, use the **Set-CsDialInConferencingAccessNumber** cmdlet.

The following command modifies the DisplayName property for the dial-in conferencing access number with the Identity sip:RedmondDialIn@litwareinc.com. In this example, the display name is set to "Redmond Dial-In Access Number":

```
Set-CsDialInConferencingAccessNumber -Identity "sip:RedmondDialIn@litwareinc.com" -DisplayName "Redmond Dial-In Access Number"
```

In the next example, the dial-in conferencing access number with the Identity sip:RedmondDialIn@litwareinc.com is modified to include two regions: Redmond and Seattle. To do this, the Regions parameter is called, followed by the two regions (two string values separated by commas). Note that this command will fail unless both the Redmond and Seattle regions have already been defined in dial plans.

```
Set-CsDialInConferencingAccessNumber -Identity "sip:RedmondDialIn@litwareinc.com" -Regions "Redmond",  
"Seattle"
```

For more information, see [Set-CsDialInConferencingAccessNumber](#).

## Delete a dial-in conferencing access number

You can delete a dial-in conferencing access number by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### Delete a dial-in conferencing access number by using Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **Dial-in Access Number**.
4. On the page, click the dial-in number you want to delete in the list, click **Edit**, and then click **Delete**.
5. Click **OK**.

### Delete a dial-in conferencing access number by using Skype for Business Server Management Shell

To delete a dial-in conferencing access number, use the **Remove-CsDialInConferencingAccessNumber**.

The following command deletes the dial-in conferencing access number with Identity sip:RedmondDialInAccess@litwareinc.com:

```
Remove-CsDialInConferencingAccessNumber -Identity "sip:RedmondDialInAccess@litwareinc.com"
```

The next command deletes all the dial-in conferencing access numbers associated with the Northwest region:

```
Get-CsDialInConferencingAccessNumber -Region "Northwest" | Remove-CsDialInConferencingAccessNumber
```

The next command deletes all the dial-in conferencing access numbers where Italian is the primary language:

```
Get-CsDialInConferencingAccessNumber | Where-Object {$_.PrimaryLanguage -eq "it-IT"} | Remove-  
CsDialInConferencingAccessNumber
```

For more information, see [Remove-CsDialInConferencingAccessNumber](#).

# Manage PIN policies for dial-in conferencing in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Learn how to manage PIN policies for dial-in conferencing in Skype for Business Server.

Skype for Business Server users who have Active Directory Domain Services (AD DS) credentials in your organization can join dial-in conferences as authenticated users by using a personal identification number (PIN). PIN policy defines the rules for how dial-in conferencing PINs work.

If you want to use the same PIN policy for your entire organization, you can use the global PIN policy and modify it as needed. The global PIN policy defines the rules for dial-in conferencing PINs at the forest level. You can modify the global PIN policy, but you cannot delete it.

You can create a new PIN policy if you want a specific policy to apply to a site or to a certain group of users.

PIN policies apply to users from the narrowest scope to the widest scope. If you assign a user-level PIN policy to a user, those settings take precedence. If you do not assign a user policy, the site-level PIN policy applies, if it exists. If no user or site policies apply, global PIN policy provides the default settings.

## View information about PIN policies

You can view information about PIN policies by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### View information about PIN policies by using Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the PIN policy that you want to view, click **Edit**, and then click **Show details**.

### View information about PIN policies by using Skype for Business Server Management Shell

To view information about PIN policies, use the **Get-CsPinPolicy** cmdlet. For example, the following command returns information about a single PIN policy with the Identity site:Redmond:

```
Get-CsPinPolicy -Identity "site:Redmond"
```

For more information, including a complete syntax description and list of parameters, see [Get-CsPinPolicy](#).

## Modify the global PIN policy

You can modify the global PIN policy by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### Modify the global dial-in conferencing PIN policy by using Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user

rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.

2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the **Global** policy, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, in **Minimum PIN length**, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
6. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
7. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
8. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
9. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
10. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
11. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

#### **IMPORTANT**

For security reasons, Microsoft recommends that you do not allow common patterns.

12. Click **Commit**.

### **Modify the global dial-in conferencing PIN policy by using Skype for Business Server Management Shell**

To modify the global dial-in conferencing PIN policy, use the **Set-CsPinPolicy** cmdlet.

The following command changes the value of the MinPasswordLength for all the PIN policies configured for use in the organization. To do this, the command first calls the **Get-CsPinPolicy** cmdlet without any parameters in order to retrieve a collection of all the existing PIN policies. That collection is then piped to the **Set-CsPinPolicy** cmdlet, which modifies the value of the MinPasswordLength property for each policy in the collection:

```
Get-CsPinPolicy | Set-CsPinPolicy -MinPasswordLength 10
```

For more information, including a complete syntax description and list of parameters, see [Set-CsPinPolicy](#).

## Create a user or site PIN policy

You can create a user or site PIN policy by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### **Create a user or site PIN policy by using Skype for Business Server Control Panel**

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click **New**, and then do one of the following:
  - To create a user-level policy, click **User policy**. In **New PIN Policy**, in **Name**, type a name that describes the policy.
  - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the list of sites, click the site you want, and then click **OK**.
5. In the **Description** field, type a description of the PIN policy.
6. In the **Minimum PIN length** field, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
7. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
8. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
9. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
10. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
11. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
12. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

**IMPORTANT**

For security reasons, Microsoft recommends that you do not allow common patterns.

13. Click **Commit**.

### Create a user or site PIN policy by using Skype for Business Server Management Shell

To create a user or site PIN policy, use the **New-CsPinPolicy** cmdlet.

The following command creates a new PIN policy with the Identity site:Redmond. This command includes just one optional parameter, `MinPasswordLength`, which is used to set the `MinPasswordLength` property to 7. All the remaining policy properties will be configured using the default values.

```
New-CsPinPolicy -Identity "site:Redmond" -MinPasswordLength 7
```

For more information, including a complete syntax description and list of parameters, see [New-CsPinPolicy](#).

## Modify a user or site PIN policy

You can modify a user or site PIN policy by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### Modify a user or site PIN policy by using Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the PIN policy that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, modify any of the policy settings (except for the policy name, which cannot be modified).
6. Click **Commit**.

### Modify a user or site PIN policy by using Skype for Business Server Management Shell

To modify the dial-in conferencing PIN policy, use the **Set-CsPinPolicy** cmdlet.

The following command modifies the PIN policy assigned to the Redmond site. In this case, the command changes the value of the MinPasswordLength property to 10; that means that new PINs will have to contain at least 10 digits:

```
Set-CsPinPolicy -Identity site:Redmond -MinPasswordLength 10
```

For more information, including a complete syntax description and list of parameters, see [Set-CsPinPolicy](#).

## Delete a user or site PIN policy

You can delete a user or site PIN policy by using Skype for Business Server Control Panel or by using Skype for Business Server Management Shell.

### Delete a user or site PIN policy by using Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open Skype for Business Server Control Panel.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the PIN policy that you want to change, click **Edit**, and then click **Delete**.

### Delete a user or site PIN policy by using Skype for Business Server Management Shell

To delete a user or site PIN policy, use the **Remove-CsPinPolicy** cmdlet.

The following command removes all the PIN policies that have been configured at the site scope. To do this, use the **Get-CsPinPolicy** cmdlet, along with the Filter parameter, to return a collection of all the policies that have an Identity that begins with the characters "site:". This collection is then piped to the **Remove-CsPinPolicy** cmdlet,



which deletes each policy in the collection:

```
Get-CsPinPolicy -Filter "site:*" | Remove-CsPinPolicy
```

For more information, including a complete syntax description and list of parameters, see [Remove-CsPinPolicy](#).

# Manage conference join and leave announcements in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage conference join and leave announcements in Skype for Business Server.

When dial-in users join or leave a conference, the Conferencing Announcement application can announce their entrance or exit by playing a tone or saying their names. You can change how announcements work by using Skype for Business Server Management Shell and the **Set-CsDialinConferencing** cmdlet with the following parameters:

- **EnableNameRecording** - Determines whether anonymous participants are asked to record their name before entering the conference. The default value is "\$true," which means that anonymous participants are prompted to state their name when joining a conference. (Authenticated participants do not record their name because their display name is used instead.)
- **EntryExitAnnouncementsEnabledByDefault** - Indicates whether announcements are turned on or off by default. The default value is "\$false," which means that by default there are no announcements when participants join or leave a conference. The meeting organizer can override this setting when scheduling a meeting.
- **EntryExitAnnouncementsType** - Indicates the action taken whenever a participant joins or leaves a conference for which announcements are enabled. The default value is "UseNames," which means there is an announcement similar to the following: "Ken Myer has joined the conference" when announcements are turned on.

You can configure these settings at the global scope or at the site scope. Settings configured at the site scope take precedence over settings configured at the global scope.

## To modify the conference join and leave announcement behavior

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the Cs-ServerAdministrator or CsAdministrator role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialinConferencingConfiguration
```

This cmdlet retrieves information about whether participants are required to record their name when joining a conference and how Skype for Business Server responds when participants join or leave a dial-in conference.

4. Run the following at the command prompt:

```
Set-CsDialinConferencingConfiguration -Identity <identity of dial-in conferencing settings to be modified>  
[-EnableNameRecording <$true | $false>]  
[-EntryExitAnnouncementsEnabledByDefault <$true | $false>]  
[-EntryExitAnnouncementsType <UseNames | ToneOnly>]
```

In the following example, settings are configured at the site scope for Redmond. Announcements are turned on, but participants are not prompted to say their name when they join a conference. A tone is played when participants enter or leave a conference:

```
Set-CsDialInConferencingConfiguration -Identity site:Redmond
-EnableNameRecording $false
-EntryExitAnnouncementsEnabledByDefault $true
-EntryExitAnnouncementsType ToneOnly
```

For more information, including syntax and a complete list of parameters, see [Set-CsDialInConferencingConfiguration](#).

# Manage key mapping for DTMF commands in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to manage key mapping of dual-tone multi-frequency (DTMF) commands in Skype for Business Server.

Dial-in conferencing users can press keys on the telephone keypad to perform dual-tone multi-frequency (DTMF) commands. DTMF commands enable users who dial in to a conference to control conference settings (such as muting and unmuting themselves or locking and unlocking the conference) by using the keypad on their telephone.

To manage the keys used for the DTMF commands, use the Skype for Business Server Management Shell with the **Get-CsDialInConferencingDtmfConfiguration**, **Set-CsDialInConferencingDtmfConfiguration**, and **New-CsDialInConferencingDtmfConfiguration** cmdlets.

When you create new DTMF settings for sites, the site settings take precedence over the global settings.

## Manage the key mapping of DTMF commands

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the Cs-ServerAdministrator or CsAdministrator role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. To view the DTMF settings used for dial-in conferencing, run the following command at the command prompt:

```
Get-CsDialInConferencingDtmfConfiguration
```

4. To modify the DTMF settings used for dial-in conferencing, run the following cmdlet and specify the key to be pressed for each option that you want to change:

```
Set-CsDialInConferencingDtmfConfiguration [-Identity <global or site collection to be changed>]
[-AdmitAll <default key is 8>] [-AudienceMuteCommand <default key is 4>]
[-CommandCharacter <* (default) | #>] [-EnableDisableAnnouncementsCommand <default key is 9>]
[-HelpCommand <default key is 1>] [-LockUnlockConferenceCommand <default key is 7>]
[-MuteUnmuteCommand <default key is 6>] [-PrivateRollCallCommand <default key is 3>]
```

5. (Optional) To create additional sets of DTMF commands for specific sites, use the **New-CsDialInConferencingDtmfConfiguration** cmdlet with a site identity.

The following example swaps the key that is pressed to enable or disable announcements and the key that is pressed to mute and unmute all participants. Because no Identity is specified, these changes apply to the global DTMF settings:

```
Set-CsDialInConferencingDtmfConfiguration -EnableDisableAnnouncementsCommand 4 -AudienceMuteCommand 9
```

For more information, see [Get-CsDialInConferencingDtmfConfiguration](#), [Set-CsDialInConferencingDtmfConfiguration](#), and [New-CsDialInConferencingDtmfConfiguration](#).

# Configure PIN-less meeting join in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to configure the PIN-less meeting join option in Skype for Business Server.

When a dial-in caller attempts to join a meeting, the Conference Auto Attendant (CAA) service places the caller in a holding pen that is different from the Lobby — if a presenter is not already on a call, and the dial-in caller has not entered a leader PIN. The PIN-less meeting join option allows dial-in callers to join a meeting without entering a leader PIN even if they are the first person on a call.

Keep the following in mind when configuring this feature:

- Applies to private meetings only.
- Allows PSTN callers to stay in private meetings without the presence of authenticated users.
- After the setting is changed, it applies to all existing and new private meetings.
- Can be enabled either at the site of the organizer or at the global level.
- Options for who can bypass the lobby can be set for either of the following:
  - **Anyone from my Organization with Callers get in directly**
  - **Anyone (no restrictions) with Callers get in directly** (This is the default setting.)
- When configured to enable PIN-less join, the CAA service still prompts for a leader PIN. Users can join the meeting whether or not a PIN is entered. However, retaining the ability to enter a leader PIN allows a dial-in caller to authenticate as a leader and manage the meeting if necessary.

## Configure PIN-less meeting join

To enable PIN-less meeting join for your users, use the [Set-CsDialInConferencingConfiguration](#) cmdlet with the `AllowAnonymousPstnActivation` parameter as follows:

```
Set-CsDialInConferencingConfiguration -Identity < global or site:sitename> -AllowAnonymousPstnActivation $True
```

For example, the following command enables PIN-less meeting join for the site Redmond:

```
Set-CsDialInConferencingConfiguration -Identity site:Redmond -AllowAnonymousPstnActivation $True
```

For security purposes, when PIN-less meeting join is turned on, you might want to restrict anonymous users from dialing out by ensuring the `ConferencingPolicy` is set as follows:

```
Set-CsConferencingPolicy [-Identity <XdsIdentity>] -AllowAnonymousUsersToDialOut $False
```

For more information, see [Set-CsConferencingPolicy](#).

# Create conference directories in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to create conference directories in Skype for Business Server.

Conference directories maintain a mapping between the alphanumeric meeting ID that a participant uses to join a conference when using Skype for Business, and the numeric-only conference ID that a dial-in conferencing participant uses to join the conference.

## Create a conference directory

Creating multiple conference directories will ensure that conference IDs will stay short until a significant amount of conferences have been created.

In an organization with a typical number of conferences per user, we recommend that you create one conference directory for every 999 users in the pool. Using this guideline, the conference IDs can generally be kept small. However, once the number of conference directories (across the pools) exceed 9, the Conference ID length will grow to support additional conferences.

The format of a conference ID is as follows:

```
<housekeeping digit (1 digit)><conference directory (usually 1-2 digits)>  
<conference number (variable number of digits)><check digit (1 digit)>
```

To create a conference directory, use the **New-CsConferenceDirectory** cmdlet. For example, the following command creates a conference directory with the identity 42, hosted on the pool atl-cs-001.litwareinc.com:

```
New-CsConferenceDirectory -Identity 42 -HomePool "atl-cs-001.litwareinc.com"
```

For more information, see [New-CsConferenceDirectory](#).

# Send welcome email to dial-in users in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to welcome users to dial-in conferencing in Skype for Business Server.

After you configure dial-in conferencing and test to verify that it is functioning properly, you should set initial personal identification numbers (PINs) for users and notify users about the availability of the feature. You can include introductory instructions such as the initial PIN and the link to the Dial-in Conferencing Settings web page.

Typically, you use the **Set-CsClientPin** cmdlet to reset PINs, but you can use the procedure in this topic if you want to send an introductory welcome email with the PIN information. If you do not want to send the email, you can use **Set-CsClientPin** instead.

You can use the **Set-CsPinSendCAWelcomeMail** script to set the PIN and send a welcome email to a single user. By default, the script does not reset a PIN if it is already set, but you can use the Force parameter to force reset a PIN. The email message is sent using Simple Mail Transfer Protocol (SMTP).

You can create a script that runs the **Set-CsPinSendCAWelcomeMail** script iteratively to set PINs and send email to a group of users. You can modify the email template (that is, the CAWelcomeEmailTemplate.html file) to add more links to intranet pages or modify the email text.

## Set an initial PIN and send welcome email

1. Log on as a member of the RTCUniversalServerAdmins group.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following at the command prompt:

```
Set-CsPinSendCAWelcomeMail -UserUri <user identifier>
-From <email address of sender> [-Subject <subject for email message>]
[-UserEmailAddress <destination email address>]
[-Cc <email address of recipients who receive copy of email>]
[-Bcc <email address of recipients who receive blind copies>]
[-TemplatePath <path for email template>]
[-SmtpServer] <SMTP server name>
[-BodyAsPlainText] [-UseSsl]
[-Pin <new numeric PIN>] [-Force] `
[-Credential <SMTP server credentials used to send email with the specified From address>]
```

**SmtpServer** By default, the script uses the value of the reserved environment variable **\$PSEmailServer** for this parameter. If the **\$PSEmailServer** variable is not set, you must specify this parameter.

**Credential** By default, the script uses the credentials of the current user. If the current user does not have permission to send email on behalf of the specified From address, you must specify this parameter. As a general rule, specify this parameter if you do not specify your email address as the From address.

The following example creates a new PIN, and then sends a welcome email from Marco to Bob. It uses the email text from the default template and creates the email message in HTML format. The default Subject is "Welcome to Dial In Conferencing":

```
Set-CsPinSendCAWelcomeMail -UserUri "bob@contoso.com"  
-From "marco@contoso.com"
```

The next example forces a new PIN with a value of "383042650" for Bob, even though Bob had an existing PIN, and then sends a welcome email from Marco to Bob. Because the Credential parameter is specified, the person running the command is prompted to enter a password. The email is sent by using the Secure Sockets Layer (SSL):

```
Set-CsPinSendCAWelcomeMail -UserUri "bob@contoso.com"  
-From "marco@contoso.com" -Subject "Your new dial-in conferencing PIN"  
-Pin "383042650" -Force  
-Credential Admin@contoso.com -UseSsl
```



# Test dial-in conferencing in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to test dial-in conferencing in Skype for Business Server.

As final verification of your dial-in conferencing configuration, you can search for dial plans that have a dial-in conferencing region that is not used by any access number and for access numbers that have not specified a dial-in conferencing region. You should also verify that the Dial-in Conferencing Settings webpage and the dial-in access numbers work correctly.

## Find dial plans with a dial-in conferencing region that is not used by an access number

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the Cs-ServerAdministrator or CsAdministrator role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialInConferencingAccessNumber -EmptyRegion
```

This cmdlet returns all of the dial plans that have a dial-in conferencing region that is not used by an access number.

For more information, see [Get-CsDialInConferencingAccessNumber](#).

## Find access numbers without assigned regions

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the Cs-ServerAdministrator or CsAdministrator role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialInConferencingAccessNumber -Region NULL
```

This cmdlet returns all the dial-in conferencing access numbers that are not associated with a region.

For more information, see [Get-CsDialInConferencingAccessNumber](#).

## Test webpage and access numbers

To verify that the Dial-in Conferencing Settings webpage and the dial-in access numbers work correctly, you need to do the following:

- Test the Dial-in Conferencing Settings webpage by signing in to the simple URL.
- Test that access numbers work correctly for a specific pool by running the script later in this topic. This script

simulates calls to access numbers. You need the SIP address and credentials of one unified communications (UC) client that is hosted on the specific pool to use this script.

### To test access numbers for a specific pool

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the Cs-ServerAdministrator or CsAdministrator role.
2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business 2015**, and then click **Skype for Business Server Management Shell**.
3. Run the following at the command prompt:

```
$credentials = Get-Credential
User name: testuser1@contoso.com
Password: *****
Test-CsDialInConferencing -UserSipAddress sip:testuser1@contoso.com -UserCredential $credentials -
TargetFqdn <serverName>.<domainName>.com -Verbose
```

The resulting report shows either Success or Failure, along with specific diagnostic information. The -Verbose flag provides more detailed information about how many access numbers were found and details about them.

For more information, see [Test-CsDialInConferencing](#).

# Configure the meeting join page in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Learn how to configure the meeting join page in Skype for Business Server.

When a user clicks a meeting link in a meeting request, the meeting join page detects whether a Skype for Business client is already installed on the user's computer. If a client is already installed, the client opens and joins the meeting. If a client is not installed, by default the Skype for Business client opens.

## Configure the meeting join page

You can modify the behavior of the meeting join page if you want to allow users to join meetings with other versions of the client. These configuration options have been removed from the Skype for Business Server Control Panel, but you configure them by using the `Set-CsWebServiceConfiguration` cmdlet.

### Meeting Join Page `Set-CsWebServiceConfiguration` parameters

SET-CSWEBSERVICECONFIGURATION PARAMETER	DESCRIPTION
ShowJoinUsingLegacyClientLink	This parameter has been deprecated for use with the on-premises version of Skype for Business Server. If set to True, users joining a meeting by using a client application other than Skype for Business will be given the opportunity to join the meeting by using their current client application. The default value is False.
ShowAlternateJoinOptionsExpanded	This parameter has been deprecated for use with the on-premises version of Skype for Business Server. If set to True, alternate options for joining an online conference are automatically expanded and shown to users. If set to False (the default value), these options will be available, but the user will have to display the list of options for themselves.

# Skype for Business Server Management Shell

5/20/2019 • 3 minutes to read

The Skype for Business Server Management Shell provides the command line interface for server administration and management. It is built on Windows PowerShell and includes a comprehensive set of management and administration cmdlets that are specific to Skype and legacy Lync server products.

Windows PowerShell allows you to manage Microsoft applications from the command line. It includes a command-line environment, product-specific commands, and a full scripting language. Windows PowerShell was first introduced as a downloadable release for the Windows operating system late in 2006, and was incorporated as the command-line interface for manageability of Microsoft Exchange Server 2007. It has been incorporated into most of the Microsoft Server products, including Lync and Skype servers beginning with Lync Server 2010. There are over 700 Lync and Skype specific cmdlets available in the Skype for Business Server Management Shell.

## NOTE

Skype for Business cmdlet reference has moved to docs.microsoft.com. Clicking on the links below will take you to the new docs.microsoft.com page. The content is now open sourced and available for community contributions through GitHub. Interested in contributing? Check out the README in the repo here: <https://github.com/MicrosoftDocs/office-docs-powershell>

Skype for Business Server ships with more than 700 cmdlets that enable administrators to manage Skype for Business Server using the Skype for Business Server Management Shell. You can retrieve help for a cmdlet directly from the command line by typing a command similar to the following:

```
Get-Help New-CsVoicePolicy -Full
```

The preceding command retrieves the complete help available for the **New-CsVoicePolicy** cmdlet. To view help for a different cmdlet, substitute **New-CsVoicePolicy** with the name of the cmdlet for which you want to retrieve help.

To retrieve a full list of cmdlets available for managing Skype for Business Server, type the following at the shell command prompt:

```
Get-Command * -Module SkypeforBusiness -CommandType cmdlet
```

Things to know about Windows PowerShell in Skype for Business Server:

- To run the Skype for Business Server cmdlets, open the Skype for Business Server Management Shell.

### Caution

If you open a Windows PowerShell window rather than the Skype for Business Server Management Shell, by default you may not be able to run the Skype cmdlets. To run Skype for Business Server cmdlets from within Windows PowerShell, first type the following at the Windows PowerShell command prompt: >

```
Import-Module SkypeforBusiness
```

- Skype for Business Server Management Shell is automatically installed on every Skype for Business Server Enterprise Edition Front End Server or Standard Edition server.
- You can update the Skype for Business Server Management Shell help content by running the [Update-](#)

[Help](#) cmdlet. The Update-Help cmdlet downloads and installs the newest help files available for all of the modules installed on your computer, including updates to Skype for Business cmdlets.

By default, the **Update-Help** cmdlet will update all the modules installed on your Skype for Business Server. If you want to update only certain modules, you can use the *Module* parameter to limit the scope of the cmdlet. The following example updates only the Skype for Business module.

```
Update-Help -Module SkypeforBusiness
```

If you need to update the Help on servers that are not connected to the internet, you can use the [Save-Help](#) cmdlet to get the latest version of the help and save it to a location you specify. You can then use the **Update-Help** cmdlet with the *-SourcePath* parameter on servers not connected to the internet to get the updated help from the location you selected. The following example shows how to save the help files to a network file share, and then update the help for the Skype for Business module from the file share.

```
// Save the help files
Save-Help -DestinationPath \\UpdateShare\HelpDownload
// Run Update-Help against the local help files
Update-Help -Module SkypeforBusiness -SourcePath \\UpdateShare\HelpDownload
```

For more detailed information, see [About Updatable Help](#).

#### **NOTE**

If you are using PowerShell remotely you may need to allow communication through a firewall. To learn more about the ports PowerShell remoting uses, see [What Port Does PowerShell Remoting Use?](#).

# Manage authentication in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Use the following procedures to manage Skype for Business Server security and authentication.

Use the following procedures to manage Skype for Business Server security and authentication.

## In this section

- [How to use Modern Authentication \(ADAL\) with Skype for Business](#)
- [Stage AV and OAuth certificates in Skype for Business Server using -Roll in Set-CsCertificate](#)
- [Assign a server-to-server authentication certificate to Skype for Business Server](#)
- [Configure server-to-server authentication for a Skype for Business Server hybrid environment.](#)
- [Configure an on-premises partner application for Skype for Business Server](#)
- [Manage Registrar configuration settings in Skype for Business Server](#)
- [Manage Web Service configuration settings in Skype for Business Server](#)
- [Manage PIN settings in Skype for Business Server](#)
- [Manage two-factor authentication in Skype for Business Server](#)

2 minutes to read

# Stage AV and OAuth certificates in Skype for Business Server using -Roll in Set-CsCertificate

5/20/2019 • 9 minutes to read

**Summary:** Stage AV and OAuth certificates for Skype for Business Server.

Audio/Video (A/V) communications is a key component of Skype for Business Server. Features such as application sharing and audio and video conferencing rely on the certificates assigned to the A/V Edge service, specifically the A/V Authentication service.

## IMPORTANT

This new feature is designed to work for the A/V Edge service and the OAuthTokenIssuer certificate. Other certificate types can be provisioned along with the A/V Edge service and OAuth certificate type, but will not benefit from the coexistence behavior that the A/V Edge service certificate will.

The Skype for Business Server Management Shell PowerShell cmdlets used to manage Skype for Business Server certificates refers to the A/V Edge service certificate as the AudioVideoAuthentication certificate type and the OAuthServer certificate as typeOAuthTokenIssuer. For the rest of this topic and to uniquely identify the certificates, they will be referred to by the same identifier type, AudioVideoAuthentication andOAuthTokenIssuer.

The A/V Authentication service is responsible for issuing tokens that are used by clients and other A/V consumers. The tokens are generated from attributes on the certificate, and when the certificate expires, loss of connection and requirement to rejoin with a new token generated by the new certificate will result. A new feature in Skype for Business Server will alleviate this problem - the ability to stage a new certificate in advance of the old one expiring and allowing both certificates to continue to function for a period of time. This feature uses updated functionality in the Set-CsCertificate Skype for Business Server Management Shell cmdlet. The new parameter -Roll, with the existing parameter -EffectiveDate, will place the new AudioVideoAuthentication certificate in the certificate store. The older AudioVideoAuthentication certificate will still remain for issued tokens to be validated against. Beginning with putting the new AudioVideoAuthentication certificate in place, the following series of events will occur:

## TIP

Using the Skype for Business Server Management Shell cmdlets for managing certificates, you can request separate and distinct certificates for each purpose on the Edge Server. Using the Certificate Wizard in the Skype for Business Server Deployment Wizard assists you in creating certificates, but is typically of the **default** type which couples all certificate uses for the Edge Server onto a single certificate. The recommended practice if you are going to use the rolling certificate feature is to decouple the AudioVideoAuthentication certificate from the other certificate purposes. You can provision and stage a certificate of the Default type, but only the AudioVideoAuthentication portion of the combined certificate will benefit from the staging. A user involved in (for example) an instant messaging conversation when the certificate expires will need to log out and log back in to make use of the new certificate associated with the Access Edge service. Similar behavior will occur for a user involved in a Web conference using the Web Conferencing Edge service. The OAuthTokenIssuer certificate is a specific type that is shared across all servers. You create and manage the certificate in one place and the certificate is stored in the Central Management store for all other servers.

Additional detail is needed to fully understand your options and requirements when using the Set-CsCertificate cmdlet and using it to stage certificates prior to the current certificate expiring. The -Roll parameter is important, but essentially single purpose. If you define it as a parameter, you are telling Set-CsCertificate that you will be



providing information about the certificate that will be affected defined by -Type (for example AudioVideoAuthentication and OAuthTokenIssuer), when the certificate will become effective defined by -EffectiveDate.

**-Roll:** The -Roll parameter is required and has dependencies that must be supplied along with it. Required parameters to fully define which certificates will be affected and how they will be applied:

**-EffectiveDate:** The parameter -EffectiveDate defines when the new certificate will become co-active with the current certificate. The -EffectiveDate can be close to the expiry time of the current certificate, or it can be a longer period of time. A recommended minimum -EffectiveDate for the AudioVideoAuthentication certificate would be 8 hours, which is the default token lifetime for AV Edge service tokens issued using the AudioVideoAuthentication certificate.

When staging OAuthTokenIssuer certificates, there are different requirements for the lead time before the certificate can become effective. The minimum time that the OAuthTokenIssuer certificate should have for its lead time is 24 hours before the expiration time of the current certificate. The extended lead time for the coexistence is because of other server roles that are dependent on the OAuthTokenIssuer certificate (Exchange Server, for example) which has a longer retention time for certificate created authentication and encryption key materials.

**-Thumbprint:** The thumbprint is an attribute on the certificate that is unique to that certificate. The -Thumbprint parameter is used to identify the certificate that will be affected by the actions of the Set-CsCertificate cmdlet.

**-Type:** The -Type parameter can accept a single certificate usage type or a comma separated list of certificate usage types. The certificate types are those that identify to the cmdlet and to the server what the purpose of the certificate is. For example, type AudioVideoAuthentication is for use by the A/V Edge service and the AV Authentication service. If you decide to stage and provision certificates of a different type at the same time, you must consider the longest required minimum effective lead time for the certificates. For example, you need to stage certificates of type AudioVideoAuthentication and OAuthTokenIssuer. Your minimum -EffectiveDate must be the greater of the two certificates, in this case the OAuthTokenIssuer, which has a minimum lead time of 24 hours. If you do not want to stage the AudioVideoAuthentication certificate with a lead time of 24 hours, stage it separately with an EffectiveDate that is more to your requirements.

#### **To update or renew an A/V Edge service certificate with a -Roll and -EffectiveDate parameters**

1. Log on to the local computer as a member of the Administrators group.
2. Request a renewal or new AudioVideoAuthentication certificate with exportable private key for the existing certificate on the A/V Edge service.
3. Import the new AudioVideoAuthentication certificate to the Edge Server and all other Edge Server in your pool (if you have a pool deployed).
4. Configure the imported certificate with the Set-CsCertificate cmdlet and use the -Roll parameter with the -EffectiveDate parameter. The effective date should be defined as the current certificate expire time (14:00:00, or 2:00:00 PM) minus token lifetime (by default eight hours). This gives us a time that the certificate must be set to active, and is the -EffectiveDate <string>: "7/22/2015 6:00:00 AM".

#### **IMPORTANT**

For an Edge pool, you must have all AudioVideoAuthentication certificates deployed and provisioned by the date and time defined by the -EffectiveDate parameter of the first certificate deployed to avoid possible A/V communications disruption due to the older certificate expiring before all client and consumer tokens have been renewed using the new certificate.

The Set-CsCertificate command with the -Roll and -EffectiveTime parameter:

```
Set-CsCertificate -Type AudioVideoAuthentication -Thumbprint
    <thumb print of new certificate> -Roll -EffectiveDate <date and time
    for certificate to become active>
```

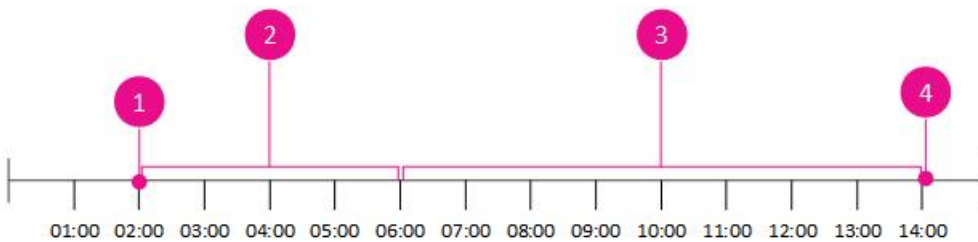
An example Set-CsCertificate command:

```
Set-CsCertificate -Type AudioVideoAuthentication -Thumbprint
    "B142918E463981A76503828BB1278391B716280987B" -Roll -EffectiveDate "7/22/2015
    6:00:00 AM"
```

### IMPORTANT

The EffectiveDate must be formatted to match your server's region and language settings. The example uses the US English Region and Language settings

To further understand the process that Set-CsCertificate, -Roll, and -EffectiveDate use to stage a new certificate for issuing new AudioVideoAuthentication tokens while still using an existing certificate to validate AudioVideoAuthentication that are in use by consumers, a visual timeline is an effective means of understanding the process. In the following example, the administrator determines that the A/V Edge service certificate is due to expire at 2:00:00 PM on 07/22/2015. He requests and receives a new certificate and imports it to each Edge Server in his pool. At 2 AM on 07/22/2015, he begins running Get-CsCertificate with -Roll, -Thumbprint equal to the thumbprint string of the new certificate, and -EffectiveTime set to 07/22/2015 6:00:00 AM. He runs this command on each Edge Server.



CALLOUT	STAGE
1	<p>Start: 7/22/2015 12:00:00 AM</p> <p>The current AudioVideoAuthentication certificate is due to expire at 2:00:00 PM on 7/22/2015. This is determined by the expires time stamp on the certificate. Plan your certificate replacement and rollover to account for an 8 hour overlap (default token lifetime) before the existing certificate reaches the expire time. The 2:00:00 AM lead time is used in this example to allow the administrator adequate time to place and provision the new certificates in advance of the 6:00:00 AM effective time.</p>
2	<p>7/22/2015 2:00:00 AM - 7/22/2015 5:59:59 AM</p> <p>Set Certificates on Edge Servers with effective time of 6:00:00 AM (4 hour lead time is for this example, but can be longer) using Set-CsCertificate -Type &lt;certificate usage type&gt; -Thumbprint &lt;thumbprint of new certificate&gt; -Roll -EffectiveDate &lt;datetime string of the effective time for new certificate&gt;</p>

COLLOUT	STAGE
3	7/22/2015 6:00 AM - 7/22/2015 2:00 PM To validate tokens, the new certificate is tried first, and if the new certificate fails to validate the token, the old certificate is tried. This process is used for all tokens during the 8 hour (default token lifetime) overlap period.
4	End: 7/22/2015 2:00:01 PM Old certificate has expired and the new certificate has taken over. Old certificate can be safely removed with Remove-CsCertificate -Type <certificate usage type> -Previous

When the effective time is reached (7/22/2015 6:00:00 AM), all new tokens are issued by the new certificate. When validating tokens, tokens will first be validated against the new certificate. If the validation fails, the old certificate is tried. The process of trying the new and falling back to the old certificate will continue until the expiry time of the old certificate. Once the old certificate has expired (7/22/2015 2:00:00 PM), tokens will only be validated by the new certificate. The old certificate can be safely removed using the Remove-CsCertificate cmdlet with the -Previous parameter.

```
Remove-CsCertificate -Type AudioVideoAuthentication -Previous
```

### To update or renew an OAuthTokenIssuer certificate with a -Roll and -EffectiveDate parameters

1. Log on to the local computer as a member of the Administrators group.
2. Request a renewal or new OAuthTokenIssuer certificate with exportable private key for the existing certificate on the Front End Server.
3. Import the new OAuthTokenIssuer certificate to a Front End Server in your pool (if you have a pool deployed). The OAuthTokenIssuer certificate is replicated globally and only needs to be updated and renewed at any server in your deployment. The Front End Server is used as an example.
4. Configure the imported certificate with the Set-CsCertificate cmdlet and use the -Roll parameter with the -EffectiveDate parameter. The effective date should be defined as the current certificate expire time (14:00:00, or 2:00:00 PM) minus a minimum of 24 hours.

The Set-CsCertificate command with the -Roll and -EffectiveTime parameter:

```
Set-CsCertificate -Type OAuthTokenIssuer -Thumbprint <thumbprint of new certificate> -Roll -EffectiveDate <date and time for certificate to become active> -identity Global
```

An example Set-CsCertificate command:

```
Set-CsCertificate -Type OAuthTokenIssuer -Thumbprint "B142918E463981A76503828BB1278391B716280987B" -Roll -EffectiveDate "7/21/2015 1:00:00 PM"
```

#### IMPORTANT

The EffectiveDate must be formatted to match your server's region and language settings. The example uses the US English Region and Language settings

When the effective time is reached (7/21/2015 1:00:00 AM), all new tokens are issued by the new certificate. When

validating tokens, tokens will first be validated against the new certificate. If the validation fails, the old certificate is tried. The process of trying the new and falling back to the old certificate will continue until the expiry time of the old certificate. Once the old certificate has expired (7/22/2015 2:00:00 PM), tokens will only be validated by the new certificate. The old certificate can be safely removed using the Remove-CsCertificate cmdlet with the -Previous parameter.

```
Remove-CsCertificate -Type OAuthTokenIssuer -Previous
```

## See also

[Manage server-to-server authentication \(OAuth\) and partner applications in Skype for Business Server](#)

[Set-CsCertificate](#)

[Remove-CsCertificate](#)

# Assign a server-to-server authentication certificate to Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Assign a server-to-server authentication certificate for Skype for Business Server.

To determine whether or not a server-to-server authentication certificate has already been assigned to Skype for Business Server, run the following command from the Skype for Business Server Management Shell:

```
Get-CsCertificate -Type OAuthTokenIssuer
```

If no certificate information is returned you must assign a token issuer certificate before you can use server-to-server authentication. As a general rule, any Skype for Business Server certificate can be used as your OAuthTokenIssuer certificate; for example, your Skype for Business Server default certificate can also be used as the OAuthTokenIssuer certificate. (The OAuthTokenIssuer certificate can also be any Web server certificate that includes the name of your SIP domain in the Subject field.) The primary two requirements for the certificate used for server-to-server authentication are these: 1) the same certificate must be configured as the OAuthTokenIssuer certificate on all of your Front End Servers; and, 2) the certificate must be at least 2048 bits.

If you do not have a certificate that can be used for server-to-server authentication you can obtain a new certificate, import the new certificate, and then use that certificate for server-to-server authentication. After you have requested and obtained the new certificate you can then log on to any one of your Front End Servers and use a Windows PowerShell command similar to this one to import and assign that certificate:

```
Import-CsCertificate -Identity global -Type OAuthTokenIssuer -Path C:\Certificates\ServerToServerAuth.pfx - Password "P@ssw0rd"
```

In the preceding command the Path parameter represents the full path to the certificate file, and the Password parameter represents the password that was assigned to the certificate. This procedure should be run just one time: the Skype for Business Server replication service will then automatically create a set of scheduled tasks that will decrypt and deploy the certificate to all your Front End Servers.

Alternatively, you can use an existing certificate as your server-to-server authentication certificate. (As noted, the default certificate can be used as the server-to-server authentication certificate.) The following pair of Windows PowerShell commands retrieve the value of the default certificate's Thumbprint property, then use that value to make the default certificate the server-to-server authentication certificate:

```
$x = (Get-CsCertificate -Type Default).Thumbprint  
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x
```

In the preceding command, the retrieved certificate is configured to function as the global server-to-server authentication certificate; that means that the certificate will be replicated to, and used by, all your Front End Servers. Again, this command should only be run one time, and only on one of your Front End Servers. Although all Front End Servers must use the same certificate, you should not configure the OAuthTokenIssuer certificate on each Front End Server. Instead, configure the certificate once, then let the Skype for Business Server replication server take care of copying that certificate to each server.

The Set-CsCertificate cmdlet takes the certificate in question and immediately configures that certificate to act as the current OAuthTokenIssuer certificate. (Skype for Business Server keeps two copies of a certificate type: the

current certificate and the previous certificate.) If you need the new certificate to immediately begin to act as the OAuthTokenIssuer certificate then you should use the Set-CsCertificate cmdlet.

You can also use the Set-CsCertificate cmdlet to "roll" a new certificate. "Rolling" a certificate simply means that you configure a new certificate to become the current OAuthTokenIssuer certificate at a specified point in time. For example, this command retrieves the default certificate and then configure that certificate to take over as the current OAuthTokenIssuer certificate as of July 1, 2015:

```
$x = (Get-CsCertificate -Type Default).Thumbprint
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x -EffectiveDate "7/1/2015" -Roll
```

On July 1, 2015, the new certificate will be configured as the current OAuthTokenIssuer certificate and the "old" OAuthTokenIssuer certificate will be configured as the previous certificate.

If you do not want to use Windows PowerShell you can also use the Certificates MMC console to export a certificate from one Front End Server and then import that same certificate on all your other Front End Servers. If you do this, make sure that you export the private key along with the certificate itself.

#### Caution

In this case, the procedure must be performed on each Front End Server. When exporting and importing certificates in this manner Skype for Business Server will not replicate that certificate to each Front End Server.

After the certificate has been imported to all your Front End Servers, that certificate can then be assigned by using the Skype for Business Server Deployment Wizard instead of Windows PowerShell. To assign a certificate by using the Deployment Wizard, complete the following steps on a computer where the Deployment Wizard has been installed:

1. Click Start, click All Programs, click **Skype for Business Server**, and then click **Skype for Business Server Deployment Wizard**.
2. In the Deployment Wizard, click **Install or Update Skype for Business Server System**.
3. On the Skype for Business Server page, click the **Run** button under the heading **Step 3: Request, Install or Assign Certificates**. (Note: If you have already installed certificates on this computer then the **Run** button will be labeled **Run Again**.)
4. In the Certificate Wizard, select the **OAuthTokenIssuer** certificate and then click **Assign**.
5. In the Certificate Assignment wizard, on the **Certificate Assignment** page, click **Next**.
6. On the **Certificate Store** page, select the certificate to be used for server-to-server authentication and then click **Next**.
7. On the Certificate Assignment Summary page, click **Next**.
8. On the Executing Commands page, click **Finish**.
9. Close the Certificate Wizard and the Deployment Wizard.

# Configure server-to-server authentication for a Skype for Business Server hybrid environment.

9/27/2019 • 4 minutes to read

**Summary:** Configure server-to-server authentication for Skype for Business Server hybrid environment.

In a hybrid configuration, some of your users are homed on an on-premises installation of Skype for Business Server while other users are homed on the Office 365 version of Skype for Business Server. In order to configure server-to-server authentication in a hybrid environment, you must first configure your on-premises installation of Skype for Business Server to trust the Office 365 authorization server. The initial step in this process can be carried out by running the following Skype for Business Server Management Shell script:

```
$TenantID = (Get-CsTenant -Filter {DisplayName -eq "Fabrikam.com"}).TenantId

$sts = Get-CsOAuthServer microsoft.sts -ErrorAction SilentlyContinue

if ($sts -eq $null)
{
    New-CsOAuthServer microsoft.sts -MetadataUrl
"https://accounts.accesscontrol.windows.net/$TenantId/metadata/json/1"
}
else
{
    if ($sts.MetadataUrl -ne "https://accounts.accesscontrol.windows.net/$TenantId/metadata/json/1")
    {
        Remove-CsOAuthServer microsoft.sts
        New-CsOAuthServer microsoft.sts -MetadataUrl
"https://accounts.accesscontrol.windows.net/$TenantId/metadata/json/1"
    }
}

$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue

if ($exch -eq $null)
{
    New-CsPartnerApplication -Identity microsoft.exchange -ApplicationIdentifier 0000002-0000-0ff1-ce00-
000000000000 -ApplicationTrustLevel Full -UseOAuthServer
}
else
{
    if ($exch.ApplicationIdentifier -ne "0000002-0000-0ff1-ce00-000000000000")
    {
        Remove-CsPartnerApplication microsoft.exchange
        New-CsPartnerApplication -Identity microsoft.exchange -ApplicationIdentifier 0000002-0000-0ff1-
ce00-000000000000 -ApplicationTrustLevel Full -UseOAuthServer
    }
    else
    {
        Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTrustLevel Full -UseOAuthServer
    }
}

Set-CsOAuthConfiguration -ServiceName 0000004-0000-0ff1-ce00-000000000000
```

Keep in mind that the realm name for a tenant is typically different than the organization name; in fact, the realm name is almost always the same as the tenant ID. Because of that, the first line in the script is used to return the value of the TenantId property for the specified tenant (in this case, fabrikam.com) and then assign that name to

the variable \$TenantId:

```
$TenantID = (Get-CsTenant -Filter {DisplayName -eq "Fabrikam.com"}).TenantId
```

To execute this script, you must have installed Skype for Business Online PowerShell module and connect to your tenant with this module. If you have not installed these cmdlets your script will fail because the Get-CsTenant cmdlet will not be available. After the script completes, you must then configure a trust relationship between Skype for Business Server and the authorization server, and a second trust relationship between Exchange 2013/2016 and the authorization server. This can only be done by using the Microsoft Online Services cmdlets.

#### NOTE

If you have not installed the Microsoft Online Services cmdlets, you will need to install it from the PowerShell repository with the cmdlet `install-module MSOnline`. Detailed information for installing and using the Microsoft Online Services Module can be found on the Office 365 web site. These instructions will also tell you how to configure single sign-on, federation, and synchronization between Office 365 and Active Directory.

After you have configured Office 365, and after you have created Office 365 service principals for Skype for Business Server and Exchange 2013, you will then need to register your credentials with these service principals. In order to do this, you must first obtain an X.509 Base64 certificate saved as a .CER file. This certificate will then be applied to the Office 365 service principals.

When you have obtained the X.509 certificate, open PowerShell console and import the Microsoft Online Windows PowerShell module containing the cmdlets that can be used to manage service principals:

```
Import-Module MSOnline
```

When the module has been imported, type the following command and then press ENTER in order to connect to Office 365:

```
Connect-MsolService
```

After you press ENTER, a credentials dialog box will appear. Enter your Office 365 user name and password in the dialog box, and then click OK.

As soon as you are connected to Office 365, you can then run the following command in order to return information about your service principals:

```
Get-MsolServicePrincipal
```

You should get back information similar to this for all your service principals:

```
ExtensionData      : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled     : True
Addresses          : {}
AppPrincipalId     : 00000004-0000-0ff1-ce00-000000000000
DisplayName        : Skype for Business Server
ObjectId           : aada5fbd-c0ae-442a-8c0b-36fec40602e2
ServicePrincipalName : SkypeForBusinessServer/litwareinc.com
TrustedForDelegation : True
```

The next step is to import, encode, and assign the X.509 certificate. To import and encode the certificate, use the



following Windows PowerShell commands, being sure to specify the complete file path to your .CER file when you call the Import method:

```
$certificate = New-Object System.Security.Cryptography.X509Certificates.X509Certificate
$certificate.Import("C:\Certificates\Office365.cer")
$binaryValue = $certificate.GetRawCertData()
$credentialsValue = [System.Convert]::ToBase64String($binaryValue)
```

After the certificate has been imported and encoded, you can then assign the certificate to your Office 365 service principals. To do that, first use the Get-MsolServicePrincipal to retrieve the value of the AppPrincipalId property for both the Skype for Business Server and the Microsoft Exchange service principals; the value of the AppPrincipalId property will be used to identify the service principal being assigned the certificate. With the AppPrincipalId property value for Skype for Business Server in hand, use the following command to assign the certificate to Skype For Business Online version:

```
New-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000 -Type Asymmetric -
Usage Verify -Value $credentialsValue
```

You should then repeat the command, this time using the AppPrincipalId property value for Exchange 2013.

If you later need to delete that certificate, for example if it has expired, you can do so by first retrieving the KeyId for the certificate:

```
Get-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000
```

That command will return data like this one:

```
Type      : Asymmetric
Value     :
KeyId     : bc2795f3-2387-4543-a95d-f92c85c7a1b0
StartDate : 6/1/2012 8:00:00 AM
EndDate   : 5/31/2013 8:00:00 AM
Usage     : Verify
```

You can then delete the certificate by using a command similar to this:

```
Remove-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000 -KeyId bc2795f3-
2387-4543-a95d-f92c85c7a1b0
```

In addition to assigning a certificate, you must also configure the Exchange Online Service Principal and configure your on-premises version of Skype for Business Server external Web services URLs as an Office 365 service principal. That can be done by carrying out the following two commands.

In the following example, Pool1ExternalWebFQDN.contoso.com is the external Web services URL for the Skype for Business Server pool. You should repeat these steps to add all the external Web services URLs in the deployment.

```
Set-MSOLServicePrincipal -AppPrincipalID 00000002-0000-0ff1-ce00-000000000000 -AccountEnabled $true
$lyncSP = Get-MSOLServicePrincipal -AppPrincipalID 00000004-0000-0ff1-ce00-000000000000
$lyncSP.ServicePrincipalNames.Add("00000004-0000-0ff1-ce00-000000000000/Pool1ExternalWebFQDN.contoso.com")
Set-MSOLServicePrincipal -AppPrincipalID 00000004-0000-0ff1-ce00-000000000000 -ServicePrincipalNames
$lyncSP.ServicePrincipalNames
```

# Configure an on-premises partner application for Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Configure an on-premises partner application for Skype for Business Server.

After you have assigned the OAuthTokenIssuer certificate you must then configure your Skype for Business Server partner applications. (The procedure about to be discussed configures both Microsoft Exchange Server 2013 and SharePoint to act as partner applications, which is optional.) To configure an on-premises partner application, you must start by copying the following Windows PowerShell script and pasting the code into Notepad (or any other text editor):

```

if ((Get-CsPartnerApplication -ErrorAction SilentlyContinue) -ne $Null)
{
    Remove-CsPartnerApplication app
}

$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue

if ($exch -eq $null)
{
    New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://at1-exchange-
001.litwareinc.com/autodiscover/metadata/json/1 -ApplicationTrustLevel Full
}
else
{
    if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-000000000000")
    {
        Remove-CsPartnerApplication microsoft.exchange
New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://at1-exchange-
001.litwareinc.com/autodiscover/metadata/json/1 -ApplicationTrustLevel Full
    }
    else
    {
        Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTrustLevel Full
    }
}

$shp = Get-CsPartnerApplication microsoft.sharepoint -ErrorAction SilentlyContinue

if ($shp -eq $null)
{
    New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl http://at1-sharepoint-
001.litwareinc.com/jsonmetadata.ashx -ApplicationTrustLevel Full
}
else
{
    if ($shp.ApplicationIdentifier -ne "00000003-0000-0ff1-ce00-000000000000")
    {
        Remove-CsPartnerApplication microsoft.sharepoint

        New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl https://at1-sharepoint-
001.litwareinc.com/_layouts/15/metadata/json/1 -ApplicationTrustLevel Full
    }
    else
    {
        Set-CsPartnerApplication -Identity microsoft.sharepoint -ApplicationTrustLevel Full
    }
}

Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000

```

After copying the code, save the script using a .PS1 file extension (for example, C:\Scripts\ServerToServerAuth.ps1). Note that, before you run this script, you must replace the metadata URLs <https://at1-exchange-001.litwareinc.com/autodiscover/metadata/json/1> and [http://at1-sharepoint-001.litwareinc.com/\\_layouts/15/metadata/json/1](http://at1-sharepoint-001.litwareinc.com/_layouts/15/metadata/json/1) with the metadata URLs used by your Exchange 2013 and SharePoint servers, respectively. See the product documentation for Exchange 2013 and SharePoint for information on how you can identify the respective product's metadata URL.

If you look at the last line of the script you will notice that the Set-CsOAuthConfiguration cmdlet is called using this syntax:

```
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

Because the Realm parameter was not used when calling Set-CsOAuthConfiguration the realm will automatically

be set to the fully qualified domain name (FQDN) of your organization (for example, litwareinc.com). If your realm name is different from your organization name then you should include the realm name, like this:

```
Set-CsOauthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000 -Realm "contoso.com"
```

After making these changes you can then execute the script, and configure both Exchange 2013 and SharePoint as partner applications, by running the script file from within the Skype for Business Server Management Shell. For example:

```
C:\Scripts\ServerToServerAuth.ps1
```

Note that you can run this script even if you do not have both Exchange 2013 and SharePoint Server installed; no problems will occur if you, say, configure SharePoint Server as a partner application even though you do not have SharePoint Server installed.

When you run this script you might receive an error message similar to the following:

```
New-CsPartnerApplication : Cannot bind parameter 'MetadataUrl' to the target. Exception setting "MetadataUrl":  
"The metadata document could not be downloaded from the URL in the MetadataUrl parameter or downloaded data is  
not a valid metadata document."
```

This error message typically means one of two things: 1) that one of the URLs specified in the script is not valid (that is, one of your metadata URLs is not an actual metadata URL); or, 2) one of the metadata URLs could not be contacted. If this happens, verify that the URLs are correct and are accessible, and the re-run the script.

After creating the partner application for Skype for Business Server you must then configure Skype for Business Server to be a partner application for Exchange 2013. You can configure partner applications for Exchange 2013 by running the script `Configure-EnterprisePartnerApplication.ps1`; all you need to do is specify the metadata URL for Skype for Business Server and indicate that Skype for Business Server is the new partner application.

To configure Skype for Business Server as a partner application for Exchange, open the Exchange Management Shell and run a command similar to this

```
"c:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartnerApplication.ps1" -  
AuthMetadataUrl "https://SkypePro.contoso.com/metadata/json/1" -ApplicationType "Lync"
```

# Manage Registrar configuration settings in Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Manage Registrar configuration settings for Skype for Business Server.

You can use the Registrar to configure proxy server authentication methods. The authentication protocol you specify determines which type of challenges the servers in the pool issue to clients. The available protocols are:

- **Kerberos** This is the strongest password-based authentication scheme available to clients, but it is normally available only to enterprise clients because it requires client connection to a Key Distribution Center (Kerberos domain controller). This setting is appropriate if the server authenticates only enterprise clients.
- **NTLM** This is the password-based authentication available to clients that use a challenge-response hashing scheme on the password. This is the only form of authentication available to clients without connectivity to a Key Distribution Center (Kerberos domain controller), such as remote users. If a server authenticates only remote users, you should choose NTLM.
- **Certificate authentication** This is the new authentication method when the server needs to obtain certificates from Lync Phone Edition clients, common area phones, Skype for Business and the Lync Windows Store app. On Lync Phone Edition clients, after a user signs in and is successfully authenticated by providing a personal identification number (PIN), Skype for Business Server then provisions the SIP URI to the phone and provisions a Skype for Business Server signed certificate or a user certificate that identifies Joe (Ex: SN=joe@contoso.com ) to the phone. This certificate is used for authenticating with the Registrar and Web Services.

## NOTE

We recommend that you enable both Kerberos and NTLM when a server supports authentication for both remote and enterprise clients. The Edge Server and internal servers communicate to ensure that only NTLM authentication is offered to remote clients. If only Kerberos is enabled on these servers, they cannot authenticate remote users. If enterprise users also authenticate against the server, Kerberos is used.

If you will use Lync Windows Store app clients, you must enable certificate authentication.

## To create new Registrar configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **Registrar**.
4. On the **Registrar** page, click **New**
5. In **Select a Service**, click the service to which the Registrar is to be applied and then click **OK**.
6. In **New Registrar Setting**, select one or more of the following depending on the capabilities of the clients and support in your environment:

- **Enable Kerberos authentication** to have the servers in the pool issue challenges using Kerberos authentication.
- **Enable NTLM authentication** to have the servers in the pool issue challenges using NTLM.
- **Enable certificate authentication** to have the servers in the pool issue certificates to clients.

7. Click **Commit**.

## Modify existing Registrar configuration settings

You can use the Registrar to configure proxy server authentication protocols.

### NOTE

We recommend that you enable both Kerberos and NTLM when a server supports authentication for both remote and enterprise clients. The Edge Server and internal servers communicate to ensure that only NTLM authentication is offered to remote clients. If only Kerberos is enabled on these servers, they cannot authenticate remote users. If enterprise users also authenticate against the server, Kerberos is used.

Follow these steps to modify an existing Registrar.

### To modify existing registrar configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **Registrar**.
4. On the **Registrar** page, click a service, click **Edit**, and then click **Show details**.
5. In **Edit Registrar Setting**, select one or more of the following depending on the capabilities of the clients and support in your environment:
  - **Enable Kerberos authentication** to have the servers in the pool issue challenges using Kerberos authentication.
  - **Enable NTLM authentication** to have the servers in the pool issue challenges using NTLM.
  - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
6. Click **Commit**.

### To delete Registrar configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **Registrar**.
4. On the **Registrar** page, and in the search field, type all or part of the name of the Registrar you want to delete.

5. In the list, click the Registrar that you want, click **Edit**, and then click **Delete**.

6. Click **OK**.

## Removing Registrar Configuration Settings by Using Windows PowerShell Cmdlets

You can delete the Registrar configuration settings by using Windows PowerShell and the **Remove-CsProxyConfiguration** cmdlet. You can run this cmdlet from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To remove a specific set of Registrar security settings

- The following command removes the Registrar security settings applied to the edge Server atl-edge-011.litwareinc.com:

```
Remove-CsProxyConfiguration -Identity service:EdgeServer:atl-edge-011.litwareinc.com
```

### To remove all of the Registrar security settings applied to the site scope

- The following command removes all the Registrar security settings applied to the Registrar service:

```
Get-CsProxyConfiguration -Filter "service:Registrar:*" | Remove-CsProxyConfiguration
```

### To remove all of the Registrar security settings that allow NTLM authentication

- The following command deletes all the Registrar security settings that allow the use of NTLM for client authentication:

```
Get-CsProxyConfiguration | Where-Object {$_.UseNtlmForClientToProxyAuth -eq $True} | Remove-CsProxyConfiguration
```

For details, see [Remove-CsProxyConfiguration](#).

# Manage Web Service configuration settings in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Manage Web Service configuration settings in Skype for Business Server.

You can use the **Web Service** page to configure the authentication methods for accessing Skype for Business Server related web servers and Web Services.

Follow these steps to create a new Web Service policy.

## To create new web service configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **Web Service**.
4. On the **Web Service** page, click **New**, and then do one of the following:
  - To configure the Web Service for a site, click **Site configuration**. In **Select a Site**, click the site to which the Web Service policy will be applied a site and click **OK**.
  - To configure the Web Service for a pool, click **Pool configuration**. In **Select a Service**, click the service to which the Web Service policy will be applied and click **OK**.
5. In **New Web Service Setting**, in **Integrated Windows authentication**, select **Negotiate**, **Integrated Windows authentication**, or **None**.
6. Select one or more of the following depending on the capabilities of the clients and support in your environment:
  - **Enable PIN Authentication** to enable clients to be authenticated using PIN numbers.
  - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
  - **Enable certificate chain download** to have servers presented with an authentication certificate download the certificate chain for that certificate.
7. Click **Commit**.

## Modify existing Web Service configuration settings

You can use the **Web Service** page to configure the authentication methods for accessing Skype for Business Server related web servers and Web Services.

Follow these steps to modify an existing Web Service policy.

## To modify existing Web service configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in



the network in which you deployed Skype for Business Server.

2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **Web Service**.
4. On the **Web Service** page, click a configuration, click **Edit**, and then click **Show details**.
5. In **Edit Web Service Setting**, in **Integrated Windows authentication**, select **Negotiate**, **Integrated Windows authentication**, or **None**.
6. Select one or more of the following depending on the capabilities of the clients and support in your environment:
  - **Enable PIN Authentication** to enable clients to be authenticated using PIN numbers.
  - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
  - **Enable certificate chain download** to have servers presented with an authentication certificate download the certificate chain for that certificate.
7. Click **Commit**.

## Delete existing Web Service configuration settings

Follow these steps to delete web service configuration settings.

### To delete web service configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **Web Service**.
4. On the **Web Service** page, and in the search field, type all or part of the name of the policy you want to delete.
5. In the list of policies, click the policy that you want, click **Edit**, and then click **Delete**.
6. Click **OK**.

## Deleting Web Service Configuration Settings by Using Windows PowerShell Cmdlets

You can delete web service configuration settings by using Windows PowerShell and the **Remove-CsWebServiceConfiguration** cmdlet. You can run this cmdlet from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To delete a specific collection of web service configuration settings

- The following command removes the Web Service security settings applied to the Redmond site:

```
Remove-CsWebServiceConfiguration -Identity "site:Redmond"
```

### To delete all of the web service configuration settings applied to the site scope

The following command removes all of the Web Service security settings applied to the service scope:

```
Get-CsWebServiceConfiguration -Filter "service:*" | Remove-CsWebServiceConfiguration
```

### To delete all of the web service configuration settings that allow certificate authentication

The following command removes all the Web Service security settings that allow the use of certificate authentication:

```
Get-CsWebServiceConfiguration | Where-Object {$_.UseCertificateAuth -eq $True} | Remove-CsWebServiceConfiguration
```

For details, see [Remove-CsWebServiceConfiguration](#).

# Manage PIN settings in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Manage PIN settings in Skype for Business Server.

Use the procedures in the following sections to manage PINs in Skype for Business Server.

You can manage Skype for Business Server PIN policies from either Skype for Business Server Control Panel or Skype for Business Server Management Shell. Use the following procedures to configure PIN policies for your organization.

- [View PIN policy information in Skype for Business Server](#)
- [Create a new PIN policy in Skype for Business Server](#)
- [Modify an existing PIN policy in Skype for Business Server](#)
- [Delete a PIN policy in Skype for Business Server](#)
- [Assign a per-user PIN policy in Skype for Business Server](#)

Use the following procedures to manage users' dial-in conferencing PINs from the **Users** section of Skype for Business Server Control Panel.

- [Set a user's dial-in conferencing PIN in Skype for Business Server](#)
- [View user PIN information in Skype for Business Server](#)
- [Lock or unlock a user PIN in Skype for Business Server](#)

# View PIN policy information in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** View a user's PIN policy information for Skype for Business Server.

You can use the **PIN Policy** tab to view personal identification number (PIN) authentication of users who are connecting to Skype for Business with IP Phones. To use PIN authentication, make sure that **Enable PIN Authentication** is selected in Web Service settings.

Follow these steps to modify a user-level or a site-level PIN policy.

## To view information about a PIN policy in Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, click a policy, click **Edit**, and then click **Show details**.

## Viewing PIN Policies by Using Windows PowerShell Cmdlets

You can also view PIN policies by using Windows PowerShell and the Get-CsPinPolicy cmdlet. This cmdlet can be run either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To view PIN policies

To view information about all your PIN policies, type the following command in the Skype for Business Server Management Shell and then press ENTER:

```
Get-CsPinPolicy
```

That will return information similar to this:

```
Identity           : Global
Description        :
MinPasswordLength  : 5
PINHistoryCount    : 0
AllowCommonPatterns : False
PINLifetime        : 0
MaximumLogonAttempts :
```

For more information, see the help topic for the [Get-CsPinPolicy](#) cmdlet.

## See also

[Create a new PIN policy in Skype for Business Server](#)

# Create a new PIN policy in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Create a new PIN policy in Skype for Business Server.

You can use the **PIN Policy** page to provide personal identification number (PIN) authentication to users who are connecting to Skype for Business with IP Phones. To use PIN authentication, make sure that **Enable PIN Authentication** is selected in Web Service settings.

Follow these steps to create a user-level or a site-level PIN policy.

## To create a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, click **New**, and then do one of the following:
  - To create a user-level policy, click **User policy**. In **New PIN Policy**, in **Name**, type a name that describes the policy.
  - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the resulting list of sites, click the site you want, and then click **OK**.
5. In the **Description** field, type a description of the PIN policy.
6. In the **Minimum PIN length** field, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
7. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
8. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
9. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
10. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
11. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
12. To allow common patterns of digits in PINs, such as "1234" and "8888", select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

**IMPORTANT**

We recommend that you do not allow common patterns.

13. Click **Commit**.

# Modify an existing PIN policy in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Modify an existing PIN policy in Skype for Business Server.

You can use the **PIN Policy** tab to provide personal identification number (PIN) authentication to users who are connecting to Skype for Business with IP Phones. To use PIN authentication, make sure that **Enable PIN Authentication** is selected in Web Service settings.

Follow these steps to modify a user-level or a site-level PIN policy.

## To modify an existing PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, click a policy, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, in **Minimum PIN length**, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
6. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
7. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
8. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
9. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
10. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
11. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

### IMPORTANT

We recommend that you do not allow common patterns.

12. Click **Commit**.



# Delete a PIN policy in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Delete a user's dial-in conferencing PIN for Skype for Business Server.

Follow these steps to delete a personal identification number (PIN) policy.

## NOTE

You cannot delete the global PIN policy.

### To delete a PIN policy in Skype for Business Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, and in the search field, type all or part of the name of the policy you want to delete.
5. In the list of policies, click the policy that you want, click **Edit**, and then click **Delete**.
6. Click **OK**.

## Removing PIN Policies by Using Windows PowerShell Cmdlets

You can delete PIN policies by using Windows PowerShell and the Remove-CsPinPolicy cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To remove a specific PIN policy

- This command removes the PIN policy with the Identity RedmondPinPolicy:

```
Remove-CsPinPolicy -Identity "RedmondPinPolicy"
```

### To remove all the PIN policies applied to the site scope

- This command removes all the PIN policies configured at the site scope:

```
Get-CsPinPolicy -Filter "site:*" | Remove-CsPinPolicy
```

### To remove all the PIN policies that allow the use of common patterns

- And this one removes all the PIN policies that allow the use of common patterns:G

```
et-CsPinPolicy | Where-Object {$_.AllowCommonPatterns -eq $True} | Remove-CsPinPolicy
```

For more information, see the help topic for the [Remove-CsPinPolicy](#) cmdlet.

# Assign a per-user PIN policy in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Stage AV and OAuth certificates for Skype for Business Server.

The dial-in conferencing personal identification number (PIN) policy is one of the individual settings of a user account that can be configured in the Skype for Business Server Control Panel.

Deploying one or more per-user PIN policies is optional. You can also deploy only a global-level PIN policy or site-level PIN policy. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact object. User rights and permissions regarding the use of PINs for dial-in conferencing automatically default to those defined in the global-level PIN policy when no specific site-level or per-user policy is assigned.

After creating at least one per-user PIN policy, use the procedures in this topic to assign the policy that specifies the constraints you want the server to impose on the PINs created by and used by a particular user.

## To assign a per-user PIN policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
  2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
  3. In the left navigation bar, click **Users**.
  4. Use one of the following methods to locate a user:
    - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
    - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
  5. (Optional) Specify additional search criteria to narrow the results:
    - a. Click **Add Filter**.
    - b. Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
    - c. In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
    - d. Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.
- TIP**  
To add additional search clauses to your query, click **Add Filter**.
- e. Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

**TIP**

If you want the same per-user PIN policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **PIN policy**, do one of the following:

**NOTE**

Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

- Allow Skype for Business Server to automatically choose either the global-level policy or, if defined, the site-level policy.
- Click the name of a per-user PIN policy you previously defined on the **PIN Policy** page.

**TIP**

To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

## Assigning a Per-User PIN Policy by Using Windows PowerShell Cmdlets

You can assign per-user PIN policies by using Windows PowerShell and the **Grant-CsPinPolicy** cmdlet. You can run this cmdlet from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To assign a per-user PIN policy to a single user

- The following command assigns the per-user PIN policy RedmondPinPolicy to the user Ken Myer.

```
Grant-CsPinPolicy -Identity "Ken Myer" -PolicyName "RedmondPinPolicy"
```

### To assign a per-user PIN policy to multiple users

- The following command assigns the per-user PIN policy RedmondUsersPinPolicy to all the users who work in the city of Redmond. For details about the LdapFilter parameter used in this command, see [Get-CsUser](#).

```
Get-CsUser -LdapFilter "l=Redmond" | Grant-CsPinPolicy -PolicyName "RedmondUsersPinPolicy"
```

### To unassign a per-user PIN policy

- The following command unassigns any per-user PIN policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsPinPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see [Grant-CsPinPolicy](#).

## See also

[Create a new PIN policy in Skype for Business Server](#)

# Set a user's dial-in conferencing PIN in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Set a user's dial-in conferencing PIN for Skype for Business Server.

To join a dial-in conference as an authenticated user, a Skype for Business Server user with Active Directory Domain Services (AD DS) credentials requires a personal identification number (PIN). If a user forgets the dial-in conferencing PIN or has not set the PIN by using Skype for Business Server, you can set the user's PIN from Skype for Business Server Control Panel. You can automatically generate the PIN or create one manually.

## NOTE

Specific characteristics of the PIN, such as its minimum length, can be configured as a policy. In addition to the global policy, you can configure a PIN policy for individual sites or users.

## To set a user's PIN

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
  - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
  - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
  - a. Click **Add Filter**.
  - b. Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
  - c. In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
  - d. Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

## TIP

To add additional search clauses to your query, click **Add Filter**.

- e. Click **Find**.

#### NOTE

If the PIN is locked, you must unlock the PIN before you can set it. To unlock the PIN, click the user, click **Action**, and then click **Unlock PIN**.

6. Click a user in the search results, click **Action**, and then click **Set PIN**.
7. In the **Set PIN** dialog box, do one of the following:
  - To allow Skype for Business Server to generate the user's PIN, select **Automatically generate a valid PIN** (the default).
  - To create your own PIN, click **Manually enter a specific PIN**, click the text box, and then type a PIN that meets the PIN requirements specified in your PIN policy settings.
8. Click **OK**.
9. In **Set PIN**, do one of the following:
  - Select the **Show PIN** check box to see the PIN, and then copy the PIN and communicate it to the user using your organization's preferred method.
  - Click **Open my email application to send the new PIN to the user** to send the PIN by email. If Microsoft Office Outlook is your email client, the PIN is automatically copied into a new email message. If you use a different email client, select the **Show PIN** check box to see the PIN and then copy it into your email message.
10. Click **Close**.

## Assigning a User PIN by Using Windows PowerShell Cmdlets

You can assign PIN numbers can also be assigned by using the Set-CsClientPin cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To auto-assign a PIN number to a user

The following command assigns a PIN number to the user Ken Myer. Because the Pin parameter is not included, Skype for Business Server will automatically generate and assign the PIN number.

```
Set-CsClientPin -Identity "Ken Myer"
```

### To assign a specific PIN number to a user

This command uses the Pin parameter to assign the PIN number 121989 to the user Ken Myer.

```
Set-CsClientPin -Identity "Ken Myer" -Pin 121989
```

For more information, see the help topic for the [Set-CsClientPin](#) cmdlet.

# View user PIN information in Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** View user PIN information in Skype for Business Server.

To join a dial-in conference as an authenticated user, a Skype for Business Server user with Active Directory Domain Services (AD DS) credentials requires a personal identification number (PIN). You can view a user's PIN information from Skype for Business Server Control Panel.

## NOTE

You can view PIN status information such as whether the PIN has been set or when the PIN was last changed, but you cannot see the current PIN by looking at the PIN status. If a user has lost their PIN, you can reset it by following the procedures in [Set a user's dial-in conferencing PIN in Skype for Business Server](#)

## To view a user's PIN in Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
  - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
  - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
  - a. Click **Add Filter**.
  - b. Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
  - c. In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
  - d. Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

## TIP

To add additional search clauses to your query, click **Add Filter**.

- e. Click **Find**.



#### NOTE

If the PIN is locked, you must unlock the PIN before you can set it. To unlock the PIN, click the user, click **Action**, and then click **Unlock PIN**.

6. Click a user in the search results, click **Action**, and then click **View PIN status**.

## Viewing User PIN Information by Using Windows PowerShell cmdlets

You can view user PIN information by using the `Get-CsClientPinInfo` cmdlet. This cmdlet can be run either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To view user PIN information

To view PIN information for a user, type a command similar to the following in the Skype for Business Server Management Shell and then press ENTER:

```
Get-CsClientPinInfo -Identity "Ken Myer"
```

That will return information similar to this:

```
Identity           : sip:kenmyer@litwareinc.com
IsPinSet           : False
IsLockedOut        : False
LastPinChangeTime  : 9/25/2012 1:35:03 PM
PinExpirationTime  :
```

For more information, see the help topic for the [Get-CsConferenceDisclaimer](#) cmdlet.

## See also

[Set a user's dial-in conferencing PIN in Skype for Business Server](#)

[Lock or unlock a user PIN in Skype for Business Server](#)

# Lock or unlock a user PIN in Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Lock or unlock a user's dial-in conferencing PIN for Skype for Business Server.

You can lock or unlock a user's PIN from the **Users** section of Skype for Business Server Control Panel.

## To lock a user's PIN in Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
  - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
  - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
  - a. Click **Add Filter**.
  - b. Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
  - c. In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
  - d. Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

### TIP

To add additional search clauses to your query, click **Add Filter**.

- e. Click **Find**.
- f. Click the user, click **Action**, and then click **Lock PIN**.

## To unlock a user's PIN in Skype for Business Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:

- In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
  - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
- a. Click **Add Filter**.
  - b. Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
  - c. In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
  - d. Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

**TIP**

To add additional search clauses to your query, click **Add Filter**.

- e. Click **Find**.
- f. Click the user, click **Action**, and then click **Unlock PIN**.

## Locking and Unlocking User PINs by Using Windows PowerShell Cmdlets

You can lock and unlock user PINs by using Windows PowerShell and the `Lock-CsClientPin` and `Unlock-CsClientPin` cmdlets. You can run these cmdlets either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To lock a user PIN

- To lock a user's PIN, use the `Lock-CsClientPin` cmdlet. For example:

```
Lock-CsClientPin -Identity "Ken Myer"
```

### To unlock a user PIN

- To unlock a user's PIN, use the `Unlock-CsClientPin` cmdlet. For example:

```
Unlock-CsClientPin -Identity "Ken Myer"
```

For more information, see the help topic for the [Lock-CsClientPin](#) and [Unlock-CsClientPin](#) cmdlets.

# Manage two-factor authentication in Skype for Business Server

5/20/2019 • 4 minutes to read

**Summary:** Manage two-factor authentication in Skype for Business Server.

Two-factor authentication provides improved security by requiring users to provide two forms of authentication or identification, namely a user name/password combination and a token or certificate. This is also known as "something you have, something you know."

A typical example of two-factor authentication with a certificate is the use of smart cards. A smart card contains a certificate associated with the user account, and can be validated against user and certificate information stored on a server. By comparing the user information (user name and password) to the certificate provided, the server validates the credentials and authenticates the user.

Consider the following subjects when configuring a Skype for Business Server environment to support two-factor authentication.

## Client Support

The Cumulative Updates for Lync Server 2013: July 2013 desktop client and the Skype for Business client are the only clients that currently support two-factor authentication.

## Topology Requirements

Customers are strongly encouraged to deploy two-factor authentication using dedicated Skype for Business Server with Edge, Director, and User Pools. To enable passive authentication for users, other authentication methods must be disabled for other roles and services, including the following:

CONFIGURATION TYPE	SERVICE TYPE	SERVER ROLE	AUTHENTICATION TYPE TO DISABLE
Web Service	WebServer	Director	Kerberos, NTLM, and Certificate
Web Service	WebServer	Front End	Kerberos, NTLM, and Certificate
Proxy	EdgeServer	Edge	Kerberos and NTLM
Proxy	Registrar	Front End	Kerberos and NTLM

Unless these authentication types are disabled at the service level, all other versions of the client will be unable to sign in successfully once two-factor authentication is enabled within in your deployment.

## Skype for Business Service Discovery

DNS records used by internal and/or external clients to discover Skype for Business services should be configured to resolve to a Skype for Business server that is not enabled for two-factor authentication. With this configuration, users from Skype for Business Pools that are not enabled for two-factor authentication will not be required to enter a PIN to authenticate, while users from Skype for Business Pools that are enabled for two-factor

authentication will be required to enter their PIN to authenticate.

## Exchange Authentication

Customers who have deployed two-factor authentication for Microsoft Exchange may find that certain features in the client are unavailable. This is currently by design, as the Skype for Business client does not support two-factor authentication for features that are dependent on Exchange integration.

## Contacts

Skype for Business users who are configured to leverage the Unified Contact Store feature will find that their contacts are no longer available after signing in with two-factor authentication.

You should use the **Invoke-CsUcsRollback** cmdlet to remove existing user contacts from the Unified Contact Store and store them in Skype for Business Server before enabling two-factor authentication.

## Skill Search

Customers who have configured the Skill Search feature in their Skype for Business environment will find that this feature does not work when Skype for Business is enabled for two-factor authentication. This is by design, as Microsoft SharePoint does not currently support two-factor authentication.

## Credentials

There are a number of deployment considerations involving saved Skype for Business credentials which may impact users who are configured to use two-factor authentication.

### Deleting Saved Credentials

Users should use the **Delete my sign-in info** option in the Skype for Business client and delete their SIP profile folder from %localappdata%\Microsoft\Office\15.0\Skype for Business before attempting to sign for the first time using two-factor authentication.

### DisableNTCredentials

With the Kerberos or NTLM authentication method, the user's Windows credentials are used automatically for authentication. In a typical Skype for Business Server deployment where Kerberos and/or NTLM is enabled for authentication, users should not have to enter their credentials every time that they sign in.

If users are unintentionally prompted for credentials before they are prompted to enter their PIN, the **DisableNTCredentials** registry key may be unintentionally configured on client computers, possibly through Group Policy.

To prevent the additional prompt for credentials, create the following registry entry on the local workstation or use the Skype for Business administrative template to apply to all users for a given pool using Group Policy:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\15.0\Lync  
  
REG_DWORD: DisableNTCredentials  
  
Value: 0x0
```

### SavePassword

When a user signs in to Skype for Business for the first time, the user is prompted to save his or her password. If selected, this option allows the user's client certificate to be stored in the personal certificate store and the user's Windows credentials to be stored in the Credential Manager of the local computer.

The **SavePassword** registry setting should be disabled when Skype for Business is configured to support two-factor authentication. To prevent users from saving their passwords, change the following registry entry on the local workstation or use the Skype for Business administrative template to apply to all users for a given pool using Group Policy:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync  
  
REG_DWORD: SavePassword  
  
Value: 0x0
```

## AD FS 2.0 Token Replay

AD FS 2.0 provides a feature referred to as token replay detection, by which multiple token requests using the same token can be detected and then discarded. When this feature is enabled, token replay detection protects the integrity of authentication requests in both the WS-Federation passive profile and the SAML WebSSO profile by making sure that the same token is never used more than once.

This feature should be enabled in situations where security is a very high concern such as when using kiosks. For more information about token replay detection, see [Best Practices for Secure Planning and Deployment of AD FS 2.0](#).

## External User Access

Configuring an ADFS Proxy or Reverse Proxy to support Skype for Business two-factor authentication from external networks is not covered in these topics.

## See also

[Configure two-factor authentication in Skype for Business Server](#)

# Configure two-factor authentication in Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Configure two-factor authentication in Skype for Business Server.

The following sections describe the steps necessary to configure two-factor authentication for your deployment. For more information about Two-factor authentication, see [Enabling Office 365 multi-factor authentication for online administrators - Grid User Post](#).

## Configure an Enterprise Root Certificate Authority to Support Smart Card Authentication

The following steps describe how to configure an Enterprise Root CA to support Smart Card Authentication:

For information on how to install an Enterprise Root CA, see [Install an Enterprise Root Certification Authority](#).

1. Log in to the Enterprise CA computer using a Domain Admin account.
2. Launch System Manager, and verify that the Certificate Authority Web Enrollment role is installed.
3. From the **Administrative Tools** menu, open the **Certification Authority** management console.
4. In the Navigation pane, expand **Certification Authority**.
5. Right click on **Certificate Templates**, select **New**, then select **Certificate Template to Issue**.
6. Select **Enrollment Agent, Smartcard User**, and **Smartcard Logon**.
7. Click **OK**.
8. Right click on **Certificate Templates**.
9. Select **Manage**.
10. Open the properties of the Smartcard User template.
11. Click on the **Security** tab.
12. Change the permissions as follows:
  - Add individual user AD accounts with Read/Enroll (Allow) permissions, or
  - Add a security group containing smart card users with Read/Enroll (Allow) permissions, or
  - Add the Domain Users group with Read/Enroll (Allow) permissions

## Configure Windows 8 for Virtual Smart Cards

One factor to consider when deploying two-factor authentication and smart card technology is the cost of implementation. Windows 8 provides a number of new security capabilities, and one of the most interesting new features is support for virtual smart cards.

For computers equipped with a Trusted Platform Module (TPM) chip that meets specification version 1.2, organizations can now get the benefits of smart card logon without making any additional investments in hardware. For more information, see [Using Virtual Smart Cards with Windows 8](#).

## To Configure Windows 8 for Virtual Smart Cards

1. Log in to the Windows 8 computer using the credentials of a Skype for Business-enabled user.
2. At the Windows 8 Start screen, move your cursor to the bottom right corner of the screen.
3. Select the **Search** option, and then search for Command Prompt.
4. Right click on **Command Prompt**, and then select **Run as Administrator**.
5. Open the Trusted Platform Module (TPM) Management console by running the following command:

```
Tpm.msc
```

6. From the TPM management console, verify that your TPM specification version is at least 1.2

### NOTE

If you receive a dialog stating that a Compatible Trust Platform Module (TPM) cannot be found, verify that the computer has a compatible TPM module and that it is enabled in the system BIOS.

7. Close the TPM management console
8. From the command prompt, create a new virtual smart card using the following command:

```
TpmVscMgr create /name MyVSC /pin default /adminkey random /generate
```

```
> [!NOTE]  
> To provide a custom PIN value when creating the virtual smart card, use /pin prompt instead.
```

9. From the command prompt, open the Computer Management console by running the following command:

```
CompMgmt.msc
```

10. In the Computer Management console, select **Device Management**.
11. Expand **Smart card readers**.
12. Verify that the new virtual smart card reader has been created successfully.

## Enroll users for smart card authentication

There are generally two methods for enrolling users for smart card authentication. The easier method involves having users enroll directly for smart card authentication using web enrollment, while the more complex method involves using an enrollment agent. This topic focuses on self-enrollment for smartcard certificates.

For more information on enrolling on behalf of users as an enrollment agent, see [Enroll for Certificates on Behalf of Other Users](#).

### To Enroll Users for Smart Card Authentication

1. Log in to the Windows 8 workstation using the credentials of a Skype for Business-enabled user.
2. Launch Internet Explorer.
3. Browse to the **Certificate Authority Web Enrollment** page (e.g. <https://MyCA.contoso.com/certsrv>).



**NOTE**

If you are using Internet Explorer 10, you may need to view this website in Compatibility Mode.

4. On the **Welcome** Page, select **Request a certificate**.
5. Next, select **Advanced Request**.
6. Select **Create and submit a request to this CA**.
7. Select **Smartcard User** under the **Certificate Template** section and complete the advanced certificate request with the following values:
  - **Key Options** confirm the following settings:
    - Select the **Create new key set** radio button
    - For **CSP**, select **Microsoft Base Smart Card Crypto Provider**
    - For **Key Usage**, select **Exchange** (this is the only option available).
    - For **Key Size**, enter 2048
    - Confirm that **Automatic key container name** is selected
    - Leave the other boxes unchecked.
  - Under **Additional Options** confirm the following values:
    - For **Request Format** select **CMC**.
    - For **Hash Algorithm** select **sha1**.
    - For **Friendly Name** enter Smartcard Certificate.
8. If you are using a physical smartcard reader, insert the smart card into the device.
9. Click **Submit** to submit the certificate request.
10. When prompted, enter the PIN that was used to create the virtual smart card.

**NOTE**

The default virtual smart card PIN value is '12345678'.

11. Once the certificate has been issued, click **Install this certificate** to complete the enrollment process.

**NOTE**

If your certificate request fails with the error "This Web browser does not support the generation of certificate requests," there are three possible ways to resolve the issue:

- a. Enable Compatibility View in Internet Explorer
- b. Enable the Turn on Intranet settings option in Internet Explorer
- c. Select the Reset all zones to default level setting under the Security tab in the Internet Explorer options menu.

# Configure Active Directory Federation Services (AD FS 2.0)

The following section describes how to configure Active Directory Federation Services (AD FS 2.0) to support multi-factor authentication. For information on how to install AD FS 2.0, see [AD FS 2.0 Step-by-Step and How To Guides](#).

## NOTE

When installing AD FS 2.0, do not use the Windows Server Manager to add the Active Directory Federation Services role. Instead, download and install the [Active Directory Federation Services 2.0 RTW package](#).

## To configure AD FS for two-factor Authentication

1. Log in to the AD FS 2.0 computer using a Domain Admin account.
2. Start Windows PowerShell.
3. From the Windows PowerShell command-line, run the following command:

```
add-pssnapin Microsoft.Adfs.PowerShell
```

4. Establish a partnership with each server that will be enabled for passive authentication by running the following command, replacing the server name specific to your deployment:

```
Add-ADFSRelyingPartyTrust -Name SfbPool01-PassiveAuth -MetadataURL  
https://Sfbpool01.contoso.com/passiveauth/federationmetadata/2007-06/federationmetadata.xml
```

5. From the Administrative Tools menu, launch the AD FS 2.0 Management console.
6. Expand **Trust Relationships > Relying Party Trusts**.
7. Verify that a new trust has been created for your Skype for Business Server.
8. Create and assign an Issuance Authorization Rule for your relying party trust using Windows PowerShell by running the following commands:

```
$IssuanceAuthorizationRules = '@RuleTemplate = "AllowAllAuthzRule" => issue(Type =  
"https://schemas.microsoft.com/authorization/claims/permit", Value = "true");'
```

```
Set-ADFSRelyingPartyTrust -TargetName SfbPool01-PassiveAuth  
-IssuanceAuthorizationRules $IssuanceAuthorizationRules
```

9. Create and assign an Issuance Transform Rule for your relying party trust using Windows PowerShell by running the following commands:

```
$IssuanceTransformRules = '@RuleTemplate = "PassThroughClaims" @RuleName = "Sid" c:[Type ==  
"https://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"]=> issue(claim = c);'
```

```
Set-ADFSRelyingPartyTrust -TargetName SfbPool01-PassiveAuth -IssuanceTransformRules $IssuanceTransformRules
```

10. From the AD FS 2.0 Management console, right click on your relying party trust and select **Edit Claim Rules**.

11. Select the **Issuance Authorization Rules** tab and verify that the new authorization rule was created successfully.
12. Select the **Issuance Transform Rules** tab and verify that the new transform rule was created successfully.

## Configuring AD FS 2.0 to support client authentication

There are two possible authentication types that can be configured to allow AD FS 2.0 to support authentication using smart cards:

- Forms-based authentication (FBA)
- Transport Layer Security Client Authentication

Using forms-based authentication, you can develop a web page that allows users to authenticate either by using their username/password or by using their smart card and PIN. This topic focuses on how to implement Transport Layer Security Client Authentication with AD FS 2.0. For more information about AD FS 2.0 authentication types, see [AD FS 2.0: How to Change the Local Authentication Type](#).

### To Configure AD FS 2.0 to Support Client Authentication

1. Log in to the AD FS 2.0 computer using a Domain Admin account.
2. Launch Windows Explorer.
3. Browse to C:\inetpub\adfs\ls
4. Make a backup copy of the existing web.config file.
5. Open the existing web.config file using Notepad.
6. From the Menu bar, select **Edit** and then select **Find**.
7. Search for <localAuthenticationTypes>.  
  
Note that there are four authentication types listed, one per line.
8. Move the line containing the TLSClient authentication type to the top of the list in the section.
9. Save and Close the web.config file.
10. Launch a Command Prompt with elevated privileges.
11. Restart IIS by running the following command:

```
IISReset /Restart /NoForce
```

## Configuring Skype for Business Server passive authentication

The following section describes how to configure Skype for Business Server to support passive authentication. Once enabled, users who are enabled for two-factor authentication will be required to use a physical or virtual smart card and a valid PIN to sign in using the Skype for Business client.

### NOTE

It is strongly recommended that customers enable passive authentication for Registrar and Web Services at the service level. If passive authentication is enabled for Registrar and Web Services at the global level, it will likely result in organization-wide authentication failures for users who are not signing in with the supported desktop client.

## Web Service Configuration

The following steps describe how to create a custom web service configuration for Directors, Enterprise Pools, and Standard Edition servers that will be enabled for passive authentication.

### To create a custom web service configuration

1. Log in to your Skype for Business Server Front End server using a Skype for Business administrator account.
2. Launch the Skype for Business Server Management Shell.
3. From the Skype for Business Server Management Shell command-line, create a new Web Service configuration for each Director, Enterprise Pool, and Standard Edition server that will be enabled for passive authentication by running the following command:

```
New-CsWebServiceConfiguration -Identity "Service:WebServer:SfBPool01.contoso.com" -UseWsFedPassiveAuth $true -WsFedPassiveMetadataUri https://dc.contoso.com/federationmetadata/2007-06/federationmetadata.xml
```

```
> [!CAUTION]
> The value for the WsFedPassiveMetadataUri FQDN is the Federation Service Name of your AD FS 2.0 server. The Federation Service Name value can be found in the AD FS 2.0 Management Console by right-clicking on **Service** from the navigation pane and then selecting **Edit Federation Service Properties**.
```

4. Verify that the UseWsFedPassiveAuth and WsFedPassiveMetadataUri values were set correctly by running the following command:

```
Get-CsWebServiceConfiguration -identity "Service:WebServer:SfBPool01.contoso.com" | format-list UseWsFedPassiveAuth, WsFedPassiveMetadataUri
```

5. For clients, Passive Authentication is the least preferred authentication method for webticket authentication. For all Directors, Enterprise Pools, and Standard Edition servers that will be enabled for passive authentication, all other authentication types must be disabled in Skype for Business Web Services by running the following cmdlet:

```
Set-CsWebServiceConfiguration -Identity "Service:WebServer:SfBPool01.contoso.com" -UseCertificateAuth $false -UsePinAuth $false -UseWindowsAuth NONE
```

6. Verify that all other authentication types have been successfully disabled by running the following cmdlet:

```
Get-CsWebServiceConfiguration -Identity "Service:WebServer:SfBPool01.contoso.com" | format-list UseCertificateAuth, UsePinAuth, UseWindowsAuth
```

## Proxy Configuration

When certificate authentication is disabled for Skype for Business Web Services, the Skype for Business client will use a less preferred authentication type, such as Kerberos or NTLM, to authenticate to the Registrar service. Certificate authentication is still needed to allow the client to retrieve a webticket, however, Kerberos and NTLM must be disabled for the Registrar service.

The following steps describe how to create a custom proxy configuration for Edge Pools, Enterprise Pools, and Standard Edition servers that will be enabled for passive authentication.

### To create a custom proxy configuration

1. From the Skype for Business Server Management Shell command-line, create a new proxy configuration for

each Skype for Business Server Edge Pool, Enterprise Pool, and Standard Edition server that will be enabled for passive authentication by running the following commands:

```
New-CsProxyConfiguration -Identity "Service:EdgeServer:EdgePool01.contoso.com" -  
UseKerberosForClientToProxyAuth $False -UseNtlmForClientToProxyAuth $False
```

```
New-CsProxyConfiguration -Identity "Service:Registrar:SfBPool01.contoso.com" -UseKerberosForClientToProxyAuth  
$False -UseNtlmForClientToProxyAuth $False
```

2. Verify that all other proxy authentication types have been successfully disabled by running the following command:

```
Get-CsProxyConfiguration -Identity "Service:Registrar:SfBPool01.contoso.com" | format-list  
UseKerberosForClientToProxyAuth, UseNtlmForClientToProxyAuth, UseCertificateForClientToProxyAuth
```

## See also

[Manage two-factor authentication in Skype for Business Server](#)

[Use two-factor authentication with Skype for Business client and Skype for Business Server](#)

# Use two-factor authentication with Skype for Business client and Skype for Business Server

5/20/2019 • 6 minutes to read

**Summary:** Use two-factor authentication with Skype for Business Server and Skype for Business.

## Sign in to Skype for Business for the first time

Your sign-in information is usually configured automatically when Skype for Business is installed. But the first time you use Skype for Business, you might have to manually start the client.

### To sign in for the first time

1. Log on to your organization's network.
2. Select **Start > All Programs > Skype for Business**.

You should see the sign-in screen.

- If the sign-in address box is already filled in, confirm that the address shown is correct.
- If it's not correct, or if the box is empty, enter your sign-in address (this is usually the same as your email address).
- If an empty password box is displayed, add your password.

3. Select **Sign-in**.

## Sign out of Skype for Business

When you're finished using Skype for Business, you can close the display, sign out of your session, or exit from the program, all from the File menu. The following table explains the differences in the options.

OPTION	WHAT IT DOES	HOW TO PERFORM IT
Close	<p>Closes your display but lets the Skype for Business session identified with your user ID continue to run. This is so you can continue to get notifications and interact with others.</p> <p>You can get the display back at any time by clicking the Skype for Business icon on the taskbar or the notification area at the bottom of your screen.</p>	<p>On the Skype for Business main window, do one of the following:</p> <ol style="list-style-type: none"><li>1. Select the <b>Options</b> button, then select <b>File &gt; Close</b>.</li><li>2. Click the <b>Close</b> button (X) in the upper-right corner of the window.</li></ol>

OPTION	WHAT IT DOES	HOW TO PERFORM IT
Sign out	<p>Ends the session associated with your user ID, but Skype for Business continues to run in the background. When you sign out, the sign-in window will appear.</p> <p><b>Tip:</b> Select <b>Delete my sign-in information</b> when you sign out to remove the record of your logon ID and password from the computer. Doing this might make it easier for support people to troubleshoot sign-in issues. It can also help ensure your sign-in information is more secure by making it difficult for unauthorized users to log on with your credentials.</p>	On the Skype for Business main window, select the <b>Options</b> button, then select <b>File &gt; Sign Out</b> .
Exit	<p>Ends your Skype for Business session and shuts down Skype for Business on your computer. After exiting, if you want to restart, select <b>Start &gt; All Programs &gt; Skype for Business</b>.</p>	On the Skype for Business main window, select the <b>Options</b> button, then select <b>File &gt; Exit</b> .

## Sign in to Skype for Business with a Smart Card

Some organizations now use a multi-step sign-in process, called two-factor authentication, to increase security for their users. If you're expected to use this option, you'll need a "smart card" to sign in to Skype for Business. Smart cards can be either physical or virtual:

- **Physical** About the size of a credit card. You insert it into a smart card reader when you log in.
- **Virtual** Not a physical object, but an electronic identifier that gets written to a special chip on your computer, which in essence builds the smart card into your computer. Available only for use with Windows 8 computers that contain the TPM (Trusted Platform Module) chip.

### Enroll your smart card

Before you can sign in with a smart card, the card must be "enrolled"—that is, your user credentials have to be identified with the card. This is the case whether the card is physical or virtual. This process may already been carried out by your Skype for Business Server administrator. Check with them if you're not sure whether that has been done.

#### NOTE

Since each virtual smart card is associated only with the device it's installed on, a separate card will need to be enrolled for each Windows 8 computer you use.

### To manually enroll your smart card

1. Log on to the computer you'll be running Skype for Business on.
2. Using Internet Explorer, browse to your organization's Certificate Authority Web Enrollment page.

Ask your Skype for Business Server administrator for the web address of this resource if you don't already have it. The URL will look something like this: [https://MyCA.\[yourcompanyname\].com/certsrv](https://MyCA.[yourcompanyname].com/certsrv).

**NOTE**

If you're using Internet Explorer 10, you may need to view this website in Compatibility Mode.

3. When you're prompted to log on to the certification page, log on using your domain account (rather than as administrator of your computer).
4. On the website Welcome Page, select **Request a certificate**.
5. Select **Advanced Request**.
6. Select **Create and submit a request to this CA**, then click **Next**.
7. Now you'll see a page called Smart Card Enrollment Station. Approve the request to install the ActiveX control, and then complete the Advanced Certificate Request form as follows:
  - a. Select **Smartcard user** from the **Certificate Template** dropdown list.
  - b. Select **Create new key set**.
  - c. Find the manufacturer information on the label of your smart card and select that manufacturer from the **CSP** dropdown list.
  - d. Select **CSP** as the Request Format, if it's not already selected.
  - e. Select **sha1** from the Hash Algorithm dropdown list, if it's not already selected.
  - f. Give your certificate a name you'll recognize, and click **Submit**.
8. Now insert your blank smart card into the card reader attached to the enrollment station and click **Enroll**.
9. When prompted, enter your personal identification number (PIN), and then click **OK**.

**NOTE**

If your technical support person has not given you a special PIN to use to enroll your smart card, use the default smart card PIN value, which is 12345678.

10. Select the option to force the user (you) to change the PIN the first time the smart card is used.
11. Now insert your blank smart card into the card reader attached to the enrollment station and click **Enroll**.
12. When prompted, enter your personal identification number (PIN), and then click **OK**.

**NOTE**

If your technical support person has not given you a special PIN to use to enroll your smart card, use the default smart card PIN value, which is 12345678.

13. Select the option to force the user (you) to change the PIN the first time the smart card is used.
14. Click **OK** to confirm that the certificate displayed has your information on it.
15. Once you see the notice that the certificate has been issued, click **Install this certificate** to complete the enrollment process.

**Sign in to Skype for Business with your smart card credentials**

Before you use your smart card for the first time, it's recommended that you click **Delete my sign-in info** on the



Skype for Business sign-in page. Doing this clears any sign-in credentials stored on your computer, and eliminates a possible source of error.

### To sign in to Skype for Business with your smart card credentials

1. Start the Skype for Business client.
2. On the Sign in screen, type your sign in user account name in the **Sign-in address** box, and then click **Sign In**.
3. If you are using a virtual smart card, skip this step.

If you are using a physical smart card, insert the smart card into your smart card reader and prompted to do so, and then click **OK** when the card is detected.

4. Type in the PIN number you for your smart card and then click **OK**.

#### **NOTE**

If you were not assigned a smart card PIN number by your support person, use the default value, which is 12345678.

## See also

[Manage two-factor authentication in Skype for Business Server](#)

[Configure two-factor authentication in Skype for Business Server](#)

# Video based Screen Sharing for Skype for Business Server

5/29/2019 • 7 minutes to read

Video-based Screen Sharing (VbSS) in Skype For Business Server 2015 is now available for download: [Skype for Business Server 2015 Cumulative Update KB3061064](#). VbSS is included with Skype for Business Server 2019.

Video-based Screen Sharing, or VbSS, grew out of Lync screen-sharing. The difference between VbSS and traditional screen-sharing has to do with the underlying protocols used, and what they excel at. Screen-sharing uses the remote desktop protocol (RDP), which is great at creating thousands of 1-to-1 sessions between people's computers. Newer technology, VbSS, will make use of User Datagram Protocol (UDP).

Skype for Business Server wanted to improve people's 1-to-1, and their 1-to-many (multi-party) conversations and meeting experiences. VbSS makes use of the media platform (which relies on UDP as the underlying protocol), with the goal of improving your video start times, the viewing quality of what you're watching (especially if what you're watching is moving fast), and reliability overall.

Part of the goal of improving screen-sharing is that transitions between VbSS and RDP be as seamless as possible when they occur. Since VbSS is an update to underlying technology that is used in screen sharing for Skype for Business Server, it may be difficult to detect which technology you're leveraging unless you're looking at SIP details in the network traffic, or you're sharing content that is fast moving or 3-D. If, for example, your workplace has a lot of legacy clients, RDP will still be available as a failsafe to your meetings and conversations. Skype for Business Server uses internal logic to decide which of the two methods (VbSS or traditional screen-sharing) to apply when clients connect. RDP can, and will, be substituted for VbSS when the situation calls for it, so that your viewing experience won't be interrupted.

## Planning

### VbSS pros and cons

Switching to VbSS aims to make three key improvements:

1. Make screen-sharing (up to 5%) more reliable compared to RDP alone.
2. Make the session setup and video experience faster compared to RDP alone (setup in half the time, with a 6:1 improvement in frames-per-second).
3. Works much better than RDP in low bandwidth conditions, even when sharing high motion content, such as 3-D graphics.

Please keep in mind that these numbers rely on the health and proper performance tuning of your network, and may involve networks external to your own, if your clients are on mobile devices.

You should also be aware that some fidelity/crispness of your shared content has been traded for reliability, speed, and efficiency. In most cases this will not be readily visible to users.

### Ports and protocols

#### Required server ports

SERVER ROLE	SERVICE NAME	PORT OR PORT RANGE	PROTOCOL	NOTES
-------------	--------------	--------------------	----------	-------

SERVER ROLE	SERVICE NAME	PORT OR PORT RANGE	PROTOCOL	NOTES
Front End Servers	Skype for Business Server Application Sharing service	5065	TCP	Used for incoming SIP listening requests for application sharing.
Front End Servers	Skype for Business Server Application Sharing service	49152-65535	TCP/UDP	Media port range used for application sharing.

### Required client ports

COMPONENT	PORT RANGE	PROTOCOL	NOTES
Clients	1024-65535	TCP/UDP	Application sharing.

If QoS is enabled for the following media ports and VbSS is also enabled, during a conference that includes desktop sharing the AS MCU will use the video port settings shown in bold below for the screen share traffic.

**IMPORTANT**

These settings are a special case, and these exact settings must be used when implementing both of these features. This overrides other recommended settings in the [documentation for QoS](#). For application sharing you will also need to specify ASMCUSVC.exe in the QoS GPO in addition to defining these port values.

### Application Server QoS/VbSS required settings

PROPERTY	PORT VALUE	PROTOCOL
AudioPortStart	49152	UDP
AudioPortCount	8348	UDP
<b>VideoPortStart</b>	<b>57501</b>	UDP
<b>VideoPortCount</b>	<b>8034</b>	UDP
AppSharingPortStart	40803	TCP
AppSharingPortCount	8348	TCP

### Capacity planning

Each Front End Server running Skype for Business Server 2015 Cumulative Update 2 (CU2) or later supports up to 375 participants for screen sharing using RDP (though only 250 per meeting). This capacity doesn't change post-CU3, when VbSS is introduced and used.

That being said, we've done performance and stress testing in our lab, and the following measurements should also be considered with regard to your own deployment (depending on usage, of course).

Assuming:

- You're using Skype for Business Server 2015 CU2 or later in your deployment.
- All the users in your Skype for Business Server environment have screen resolutions higher than 1920x1080.

At full capacity (which as noted above, is 375 screen sharing participants per Front End Server in total, though only 250 per meeting), your Front End Server may be utilizing ~89% of the 1 Gigabit of network card. This is because the existing screen sharing technology in Skype for Business Server CU2 (RDP) transmits the on-screen content at the native resolution of the presenter's PC. So with higher screen resolutions factored in, you may already be experiencing network bottlenecks for screen sharing with Skype for Business Server 2015 CU2.

To mitigate this, one or more of the following options may be helpful:

- Upgrade your Front End Server from a 1 Gigabit network card to a 10 Gigabit Ethernet card.
- Increase the number of Front End Servers to load-balance traffic.
- Limit the bandwidth (bitrate) used for VbSS and RDP by putting a cap on the maximum bandwidth used by either channels.

The numbers in this table are influenced by individual networks and by the content being shared. Please test to establish baselines for your network or networks.

1080P CONTENT	RDP AVERAGE	RDP PEAK	VBSS AVERAGE	VBSS PEAK
PPT	200kbps	12mbps	100kbps	3mbps
CAD	3mbps	7mbps	1mbps	3mbps
Video	5mbps	7mbps	1.3mbps	2.2mbps

### Network bandwidth requirements for media traffic

The VbSS bandwidth is:

VIDEO CODEC	RESOLUTION AND ASPECT RATIO	MAXIMUM VIDEO PAYLOAD BIT RATE (KBPS)	MINIMUM VIDEO PAYLOAD BIT RATE (KBPS)
H.264	1920x1080 (16:9) (The aspect ratio depends on the sharer's monitor resolution, and will not always be 16:9)	4000	1500

## Clients and servers support

Video-based Screen Sharing requires Skype for Business Server 2015 CU3 or later, and a current version of the supporting clients listed in [Mobile client feature comparison for Skype for Business](#) and [Meetings support](#).

There are situations where screen-sharing will transition to RDP, like these:

- If your account is hosted in an environment where the ASMCU doesn't meet the minimum build that supports VbSS.
- If someone who uses an older version of the Skype for Business client joins your session, for example anyone using any Windows client version that is lower than 16.0.6330.1000, Skype for Business Room System Devices, or Skype for Business Mobile Apps.
- If a user is sharing from the Skype for Business Web App.
- If someone is using Skype for Business on Mac and not is homed on Skype for Business Online or Skype for Business Server 2015 with the July, 2018 cumulative update (or later).
- If someone starts any Program/Windows Sharing.
- If someone starts recording the session.

- If someone invokes Remote Screen Control during the session.
- Meetings with more than 250 participants (where VbSS is not currently supported).

Be aware that once the session transitions to RDP it will not transition back to VbSS. Again, the transition from VbSS is meant to be seamless, and, with hope, will not be easy to detect in most situations.

#### NOTE

It's not supported to block, or attempt to block, transition from VbSS to RDP in Skype for Business screen-sharing.

## Enabling, disabling, and configuring VbSS

The great thing is, once you've installed the Skype for Business Server 2015 Cumulative Update 3 (CU3) or later, all your users will be enabled for 1-to-1 and multi-party VbSS by default. This may be problematic for you if you have a reason to not have this functionality enabled for all your users. In that case, you're able to use these steps to disable users (the enable users steps will follow):

### How to disable users from using VbSS

- You can assign a user policy that doesn't allow VbSS to any users who shouldn't be using VbSS by running this cmdlet in the Skype for Business Management Console (replace [PolicyName] with the policy you're doing this for):

```
Set-CsConferencingPolicy -Identity [PolicyName] -ApplicationSharingMode RDP
```

- You also can update the global conferencing policy, which will affect all users without an assigned policy:

```
Set-CsConferencingPolicy -ApplicationSharingMode RDP
```

For more information on this command, see [Set-CsConferencingPolicy](#).

- If you need to turn VbSS off completely, you can run this command:

```
Set-CsMediaConfiguration -EnableVideoBasedSharing $false
```

For more information on this command, see [Set-CsMediaConfiguration](#).

#### NOTE

In a multiparty Skype for Business meeting, all client endpoints will respect the policy setting for the meeting organizer.

### How to enable users to use VbSS

- You can assign a specific user policy that allows VbSS to any users who need to be using VbSS by running this cmdlet in the Skype for Business Management Console (replace [PolicyName] with the policy you're doing this for):

```
Set-CsConferencingPolicy -Identity [PolicyName] -ApplicationSharingMode VideoWithFallback
```

- You also can update the global conferencing policy, which will affect all users without an assigned policy:

```
Set-CsConferencingPolicy -ApplicationSharingMode VideoWithFallback
```

For more information on this command, see [Set-CsConferencingPolicy](#).

- If you need to turn VbSS back on after turning it off (it's on by default), you can run this command:

```
Set-CsMediaConfiguration -EnableVideoBasedSharing $true
```

For more information on this command, see [Set-CsMediaConfiguration](#).

**NOTE**

In a multi-party Skype for Business meeting, all client endpoints will respect the policy setting for the meeting organizer.

## See also

[Skype for Business Server 2015 Cumulative Update KB3061064](#)

[Video-based screen-sharing \(VBSS\) is available in Skype for Business Server 2015](#)

# Manage user accounts for Skype for Business Server

5/20/2019 • 8 minutes to read

The sections in this article describe how to enable, temporarily disable, or remove Active Directory users from Skype for Business Server.

For information on how to enable an Active Directory user, see [Create a New User Account](#). For information on how to delete an Active Directory user, see [Delete a User Account](#).

These procedures should be performed during a maintenance window, when Skype for Business usage is lowest. Whether this is done on a daily or weekly schedule will be determined by the needs of your organization.

This article contains the following procedures:

- [To search for one or more users](#)
- [Add and enable a new Skype for Business Server user](#)
- [Disable or re-enable a user account previously enabled for Skype for Business Server](#)
- [Disable a user for Enterprise Voice](#)
- [Remove a user account with the Skype for Business Server Management Shell](#)

## To search for one or more users

You can use the results of a search query to configure Active Directory users for Skype for Business Server. You can search for users by display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI).

You can search for users by using the Skype for Business Server Control Panel or the Active Directory Users and Computers snap-in. The following procedure describes how to use Skype for Business Server Control Panel to search for users.

### NOTE

In an environment with a central forest topology, search results might not be accurate when you search for a user by the user's email address. Instead, you can search for users by specifying a SIP address prefix, for example, sip:name, add a search filter and select a SIP address that contains a partial email address, or use the **Get-CSUser** cmdlet.

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, SAM account name, SIP address, or line URI of the user account that you want to search for, and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
  - a. Click the expand arrow button in the upper-right corner of the screen above **Search results**, and then click **Add Filter**.

- b. Enter the user property by typing it or clicking the arrow in the drop-down list to select a user property.
  - c. In the **Equal to** list, click **Equal to** or **Not equal to**.
  - d. In the text box, type the search criteria you want to use to filter search results, and then click **Find**.
6. The search results appear under **Search Results**. You can select any or all of the users in the list and perform configuration tasks on the users you select.

## Add and enable a new Skype for Business Server user

After enabling a user account in Active Directory Users and Computers, you can use Skype for Business Server Control Panel to create and enable new Skype for Business Server user accounts by adding an Active Directory user to Skype for Business Server.

You can also use a cmdlet, specifically [Enable-CsUser](#).

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. Click **Enable users**.
5. On the **New Lync Server User** dialog, click **Add**.
6. In the **Search users** box, type all or the first portion of the name, display name, first name, last name, Security Accounts Manager (SAM) account name, email address, User Principal Name (UPN), or phone number of the Active Directory user account that you want, and then click **Find**.
7. In the table, select the account you want to add to Skype for Business Server, and then click **OK**.
8. Assign the user to a pool, specify any additional details, and assign the policies to the user you want, and then click **Enable**.

## Disable or re-enable a user account previously enabled for Skype for Business Server

You can use the following procedure to disable a previously enabled user account in Skype for Business Server without losing the Skype for Business Server settings that you configured for the user account. Because you do not lose the Skype for Business Server user account settings, you can re-enable a previously enabled user account again without having to reconfigure the user account.

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to disable or re-enable, and then click **Find**.
5. In the table, click the user account that you want to disable or re-enable.



6. On the **Action** menu, do one of the following:

- To temporarily disable the user account for Skype for Business Server, click **Temporarily disable for Lync Server**.
- To enable the user account for Skype for Business Server, click **Re-enable for Lync Server**.

#### Use Windows Powershell to Disable or Re-enable User Accounts

User accounts can be temporarily disabled, and then later re-enabled, by using the **Set-CsUser** cmdlet. You can run this cmdlet either from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

#### To disable a user account

- To temporarily disable a user account, set the value of the Enabled property to False (\$False). For example:

```
Set-CsUser -Identity "Ken Myer" -Enabled $False
```

#### To re-enable a user account

- To re-enable a disabled user account, set the value of the Enabled property to True (\$True). For example:

```
Set-CsUser -Identity "Ken Myer" -Enabled $True
```

For more information, see the help topic for the [Set-CsUser](#) cmdlet.

## Disable a user for Enterprise Voice

Use the following procedure to disable Enterprise Voice for a user account that is enabled for Skype for Business Server.

#### To disable a user account for Enterprise Voice

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to enable for Enterprise Voice.
6. On the **Edit** menu, click **Show details**.
7. On the **Edit Lync Server User** page, under **Telephony**, click any option except **Enterprise Voice**.

#### NOTE

To restrict a user from making audio or video calls by using Lync, under **Telephony**, click **Audio/video disabled**.

8. Click **Commit**.

The user is now unable to use the Enterprise Voice feature. Related information:

[Enterprise Voice and mobility](#)

[Enable users for Enterprise Voice in Skype for Business Server](#)

[Skype for Business Server Management Shell](#)

## Remove a user account with the Skype for Business Server Management Shell

You can use the following procedure to remove a previously added user account in Skype for Business Server.

### NOTE

Removing a user will cause you to lose any settings you configured for the user account. If you would like to temporarily disable a user account instead, see [Disable or re-enable a user account previously enabled for Skype for Business Server](#).

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to disable or re-enable, and then click **Find**.
5. In the table, click the user account that you want to remove.
6. On the **Action** menu, select **Remove from Lync Server**, and a dialog box appears.
7. From the dialog box, select **OK** to remove the user.

### Remove user accounts with Windows Powershell cmdlets

You can remove user accounts by using the Disable-CsUser cmdlet. This cmdlet can be run either from the Skype for Business Server Management Shell or from a remote session Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To remove a user account

To remove a user account, use the Disable-CsUser cmdlet. For example:

```
Disable-CsUser -Identity "Ken Myer"
```

After this command has run there is no way to re-enable the account and its previous settings. Instead, you will need to use the Enable-CsUser cmdlet to create a brand-new account for Ken Myer.

For more information, see the help topic for the [Disable-CsUser](#) cmdlet.

## See also

[Enable-CsUser](#)

[Disable-CsUser](#)

# Customize user account properties for Skype for Business Server

6/25/2019 • 7 minutes to read

You can use the procedures in this section to modify individual user account properties.

There are two basic operations that can be done at the individual user level:

- [Configure telephony options for a specific user account](#)
- [Move users to another pool](#)

## Configure telephony options for a specific user account

You can customize the telephony settings for a specific user (so long as the individual user has been enabled for Skype for Business Server and the organization supports telephony).

Skype for Business Server user telephony options include the following:

- **Audio/video disabled** The user cannot make calls with audio and video.
- **PC-to-PC only** The user can make only PC-to-PC audio or video calls.
- **Enterprise Voice** The user can use the Skype for Business Server infrastructure to route all incoming and outgoing calls. The user can also make PC-to-PC calls.
- **Remote call control** The user can use Skype for Business Server to control the desktop phone, and can also make PC-to-PC calls.

For details about configuring telephony for an organization, see [Enable users for Enterprise Voice in Skype for Business Server](#) and [Deploy Enterprise Voice in Skype for Business Server](#) in the Deployment documentation.

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want, and then click **Find**.
5. In the table, click the user account that you want to modify.
6. On the **Edit** menu, click **Modify**.
7. In **Telephony**, do the following:
  - To disable audio and video calls for the user, click **Audio/video disabled**.
  - To enable PC-to-PC audio communications for the user, but not remote call control or Enterprise Voice, click **PC-to-PC only**. Specify a value for **Line URI** for the telephone that the user uses for PC-to-PC audio communications.

- To route the user's phone calls by using the Skype for Business infrastructure in accordance with the class of service policy, including PC-to-PC audio communication, click **Enterprise Voice**. In **Line URI**, specify the telephone number for Enterprise Voice. In **Dial plan policy** and **Voice policy**, specify the appropriate policies for the user. To specify the normalization rules for translating phone numbers dialed by the user to the E.164 format, select the appropriate location profile in **Location policy**.
- To enable remote call control, which enables users to control their desktop phone line from Skype for Business Server to make PC-to-PC calls and PC-to-phone calls, click **Remote call control**. In **Line URI**, specify the telephone number for remote call control. The user must have a desktop phone and private branch exchange (PBX) connection for call routing.

## Move users to another pool

You can use Skype for Business Server Control Panel to assign users to a specific server or pool.

### TIP

Moving all existing users from a source pool that is running Lync Server 2010 or earlier to a Skype for Business Server destination pool in a complex Active Directory environment might result in slower Active Directory replication. To avoid this, you can use search filters to move users from pools that are running Lync Server 2010 or earlier separately, or you can use Skype for Business Server Management Shell to move users with cmdlets. Also, the filter functionality works with Skype for Business Server users.

### To move selected users to a different server or pool

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want, and then click **Find**.
5. In the table, select a specific user or users in the list.
6. On the **Action** menu, click **Move selected users to pool**.
7. In **Move Users**, select the pool that you want to move the users to in **Destination registrar pool**.
8. (Optional) If the destination server or pool is unavailable, select the **Force** check box.

### Caution

If you select **Force**, the user account is moved, but any associated user data is deleted (for example, conferences that the user has scheduled). If you do not select it, both the account and the associated data are moved.

### To move all users from one server or pool to a different server or pool

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.

4. On the **Action** menu, click **Move all users to pool**.
5. In **Move Users**, select the pool that contains the user accounts that you want to move in **Source registrar pool**.
6. In **Destination registrar pool**, select the pool that you want to move the users to.
7. (Optional) If the destination server or pool is unavailable, select the **Force** check box.

**Caution**

If you select **Force**, the user account is moved, but any associated user data is deleted (for example, conferences that the user has scheduled). If you do not select it, both the account and the associated data are moved.

#### **To move users from one pool to a different pool by using a filter**

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Users**.
4. In **User Search**, click **Search**, and then click **Add Filter**.
5. In the Search criteria, select **Registrar Pool**, select **Equal to**, select **Current Pool FQDN**, and then click **Find**.
6. On the **Action** menu, click **Move all users to pool**.

**NOTE**

When a filter is applied to an existing set of users, the option **Move all users to pool** is in the context of the filtered subset of users, not **all** possible users.

7. In **Move Users**, select the pool that contains the user accounts that you want to move in **Source registrar pool**.
8. In **Destination registrar pool**, select the pool where you want to move the users.
9. (Optional) If the destination server or pool is unavailable, select the **Force** check box.

**Caution**

If you select **Force**, the user account is moved, but any associated user data is deleted (for example, conferences that the user has scheduled and contacts). If you do not select it, both the account and the associated data are moved.

#### **To move users from one pool to another using Windows Powershell cmdlets**

1. Depending on how you run Windows PowerShell commands (that is, locally or remotely), you need to log on as a member of the correct Skype for Business Server administrative roles as follows:
  - a. If you are running the commands on the local machine (for example, you log on directly to a Front End Server): Log on to the computer where Skype for Business Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in **Delegate Setup Permissions**.
  - b. If you are running the commands remotely on another computer (for example, you log on to your computer and run the commands remotely on a Standard Edition Front End Server): From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in

your internal deployment.

2. Start the Skype for Business Server Management Shell: Click **Start**, click **All Programs**, click **Skype for Business**, and then click **Skype for Business Server Management Shell**.
3. To move single users, use the Move-CsUser cmdlet as follows:

```
Move-CsUser -Identity "Pilar Ackerman" -Target "pool01.contoso.net"
```

Where the user to move is the user Pilar Ackerman, and the user will be moved from their currently assigned home pool to the pool pool01.contoso.net

4. To move a large number of users, use filters with the **Get-CsUser** cmdlet and pass the resulting set of users to **Move-CsUser**:

```
Get-CsUser -Filter {RegistrarPool -eq "CurrentPoolFqdn"} | Move-CsUser -Target "TargetPoolFQDN"
```

The combined commands of the **Get-CsUser** and **Move-CsUser** might result in this:

```
Get-CsUser -Filter {RegistrarPool -eq "pool02.contoso.net"} | Move-CsUser -Target "pool01.contoso.net"
```

# Manage services for Skype for Business Server

5/20/2019 • 6 minutes to read

This article describes how to manage services running in a Skype for Business Server topology.

## View a list of computers running Skype for Business Server

You can use Skype for Business Server Control Panel to view a list of all the computers that are running Skype for Business Server in your topology and see the service status of each. You can sort the list by computer, pool, or site.

### To view a list of computers running Skype for Business Server

1. From a user account that is assigned to any of the predefined administrative roles for Skype for Business Server, log on to any computer in your internal deployment. For details about the predefined administrative roles available in Skype for Business Server, see **Planning for Role-Based Access Control**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, do any of the following as needed:
  - Sort the list by clicking the **Computer**, **Pool**, or **Site** column heading, and then clicking the up arrow or the down arrow.
  - Click **Refresh** to view the most up-to-date list.
  - Search for a specific computer by typing the computer name in the search field.

## View the status of services running on a Skype for Business server

You can use Skype for Business Server Control Panel to view all the services that are running on a specific computer in your Skype for Business Server topology and see the status of each service.

### To view the status of services running on a computer

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology**.
4. On the **Status** page, sort or search the list, as required, to find the computer you're interested in, and then click the computer name.
5. Do any of the following:
  - To see the latest status of services running on the computer, click **Get service status**.
  - To see a list of specific services running on the computer and the status of each service, click **Properties**, and then click **Close** to return to the list.

### Viewing service status with Windows Powershell cmdlets

You can also view service status by using Windows PowerShell and the **Get-CsWindowsService** cmdlet. You can run this cmdlet from the Skype for Business Server Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Skype for Business Server, see the blog article "[Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell](#)". The process is the same in Skype for Business Server.

### To view service status

To view service status on a computer, type a command similar to the following in the Skype for Business Server

Management Shell and then press Enter:

```
Get-CsWindowsService -ComputerName atl-cs-001.litwareinc.com | Select-Object RoleName, Status
```

This command returns information similar to the following:

ROLENAME	STATUS
{W3SVC}	Running
{CentralManagement}	Running
{ClsAgent}	Running
{Registrar, UserServer, EdgeServer}	Running
{ApplicationServer}	Running
{ConferencingServer}	Running
{MediationServer}	Running

For details, see [Get-CsWindowsService](#).

## View details about a service

You can use Skype for Business Server Control Panel to view details about each service that is running on a specific computer in your topology. You can view the status of each service and details such as the associated databases, ports, and dependent services.

### To view details for a service

1. From a user account that is assigned to any of the predefined administrative roles for Skype for Business Server, log on to any computer in your internal deployment. For details about the predefined administrative roles available in Skype for Business Server, see **Planning for Role-Based Access Control**.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. In the **Status** page, sort or search through the list and then click the computer that you want to view.
5. Click **Properties**.
6. In the **View Computer Detail** window, sort the list of services, if necessary, and click the service you want to view.
7. Do any of the following as needed:
  - To see the latest status of that specific service, click **Get service status**.
  - To see the details for that specific service, click **Properties** and then click **Close**.
  - To return to the list of all computers in your topology, click **Close**.

## Start or stop Skype for Business Server services

You can use Skype for Business Server Control Panel to start or stop all the Skype for Business Server services running on a specific computer or to start or stop a specific service.

### To start or stop all Skype for Business services on a computer

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user



rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server. You can determine whether you have been assigned the CsServerAdministrator or the CsAdministrator RBAC role by running a command similar to the following:

```
Get-CsAdminRoleAssignment -Identity "kenmyer"
```

2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the services you want to start or stop, and then click it.
5. Click **Action**.
6. Click **Start All services** or **Stop All services**.

#### To start or stop a specific service

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
5. Click **Properties**.
6. Sort the list of services, if necessary, and click the service you want to start or stop.
7. Click **Action**.
8. Click **Start service** or **Stop service**.
9. Click **Close**.

## Prevent sessions for services

You can use Skype for Business Server Control Panel to prevent new sessions for all the Skype for Business Server services running on a specific computer or to prevent new sessions for a specific Skype for Business Server service.

#### To prevent new sessions for all Skype for Business services on a computer

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the services for which you want to prevent new sessions, and then click it.
5. Click **Action**.
6. Click **Prevent new sessions for all services**.

#### To prevent new sessions for a specific service

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Skype for Business Server.
2. Open a browser window, and then enter the Admin URL to open the Skype for Business Server Control Panel.

3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
5. Click **Properties**.
6. Sort the list of services, if necessary, and click the service for which you want to prevent new sessions.
7. Click **Action**.
8. Click **Prevent new sessions for service**.
9. Click **Close**.

# Back up Response Group Service (RGS) data

7/23/2019 • 2 minutes to read

With the Skype for Business Server 2019 July cumulative update, we've included the ability to include RGS data as part of the standard backup.

## RGS data replication

To try RGS data replication functionality, please follow the steps below:

1. Install the July cumulative update on all front-ends (FEs) of your paired pool.
2. Install the RGS database on both members of the paired pool:
  - `Install-CsDatabase -ConfiguredDatabases -SqlServerFqdn <Pool1 BackendDatabase FQDN>`
  - `Install-CsDatabase -ConfiguredDatabases -SqlServerFqdn <Pool2 BackendDatabase FQDN>`
3. Run the following cmdlet on both pools to replicate existing RGS Data to the backup tables so that the data can be picked up by RGSBackupService:
  - `Invoke-CsRGSStoreReplicateData -PoolFqdn <Pool1 FQDN>`
  - `Invoke-CsRGSStoreReplicateData -PoolFqdn <Pool2 FQDN>`
4. Enable RGSBackupService (This will enable RGSBackupService globally. If this parameter is set to true, RGSBackupService will start syncing RGS data on paired pools (both pools needs to be CU1). Wait for a few minutes to get it started. Initially, RGS BackupService status will be NotInitialized.):
  - `Set-CsBackupServiceConfiguration -EnableRgsBackupService 1`
5. To check BackupServiceStatus:
  - `Get-CsBackupServiceStatus -Category RGS -PoolFqdn <Pool1 FQDN>`
6. To check DataReplication across pools, use these cmdlets (These cmdlets show only owner pool data):
  - `Get-CsRGSWorkflow`
  - `Get-CsRGSQueue`
  - `Get-CsRGSAgentGroup`
  - `Get-CsRGSHourOfBusiness`
  - `Get-CsRGSHolidaySet`
7. To check Owner pool RGS data and its backup data:
  - `Get-CsRGSWorkflow -showAll`
  - `Get-CsRGSQueue -showAll`
  - `Get-CsRGSAgentGroup -showAll`
  - `Get-CsRGSHourOfBusiness -showAll`
  - `Get-CsRGSHolidaySet -showAll`
8. Verify workflow functionality by making an audio call to Workflow.
9. Failover your RGS Owner pool.
10. Verify workflow functionality by making an audio call to Workflow.
11. Failback the pool.
12. Update RGS Data on source pool and perform another failover to check that changes are reflected on backup pool. RGS should behave in same way as it was behaving before failover.

## TIP

It is recommended you perform these steps on a bulk of data and do frequent failover and failbacks. Any new RGS created after this CU update should also be replicated.

## RGS cmdlets

- To check BackupServiceStatus (The export status should be in the Final or Steady state. The import status should be in the Normal state. RGSBackupService should be enabled.):
  - `Get-CsBackupServiceStatus -Category RGS -PoolFqdn <Pool1 FQDN>`
- To Fully Sync RGS Data on the backup pool (This will sync the full RGS data on the backup pool.):
  - `Invoke-CsBackupServiceSync -PoolFqdn <Pool1 FQDN> -BackupModule ApplicationServer.RGSDataStore`
- To Fully Sync the RGS filestore on the backup pool (This will sync the full RGS data on the backup pool.):
  - `Invoke-CsBackupServiceSync -PoolFqdn <Pool1 FQDN> -BackupModule ApplicationServer.RGSFileStore`
- To Sync RGS delta data on the backup pool (This will sync delta data on backup pool for RGS only.):
  - `Backup-CsPool -PoolFqdn <Pool FQDN> -Category RGS`
- To sync all module data including RGS:
  - `Backup-CsPool -PoolFqdn <Pool FQDN>`
- To disable RGSBackupService (This will disable RGSBackupService globally. If this parameter is set to true, RGSBackupService will be disabled on all paired pools.):
  - `Set-CsBackupServiceConfiguration -EnableRgsBackupService 0`

# Using SEFAUtil functionality via PowerShell in Skype for Business Server 2019

9/10/2019 • 3 minutes to read

SEFAUtil (Secondary Extension Feature Activation) enables Skype for Business Server administrators and helpdesk agents to configure delegate-ringing, call-forwarding, and Group Call Pickup settings on behalf of a Skype for Business Server user. This tool also allows administrators to query the call-routing settings that are published for a particular user. After you install the Skype for Business Server 2019 July cumulative update, the following functionality that can currently be managed only through SEFAUtil will be also manageable through PowerShell:

- [Call forwarding settings](#)
- [Delegation settings](#)
- [Team members and related settings](#)

## Call forwarding settings

Administrators can change call forwarding settings by using the following cmdlet in PowerShell:

- `Get-CsUserCallForwardingSettings -Identity <UserIdParameter>`

This cmdlet returns the specified user's call forwarding settings as an object and displays the same on the screen.

- `Set-CsUserCallForwardingSettings -Identity <UserIdParameter> [Param1 <Value>] [Param2 <Value>]...`

This cmdlet modifies the specified user's call forwarding settings. This cmdlet returns the specified user's call forwarding settings as an object, and displays the same on the screen, in case of success. In case of failure, an appropriate error message will be shown.

- `Set-CsUserCallForwardingSettings [-Identity] <UserIdParameter> -DisableForwarding [-UnansweredToVoicemail] [-UnansweredWaitTime <TimeSpan>] [-SettingsActiveWorkHours]`
- `Set-CsUserCallForwardingSettings [-Identity] <UserIdParameter> -DisableForwarding [-UnansweredToOther <String>] [-UnansweredWaitTime <TimeSpan>] [-SettingsActiveWorkHours]`

This cmdlet disables the user's call forwarding settings (we show two different parameter examples here).

- `Set-CsUserCallForwardingSettings [-Identity] <UserIdParameter> -EnableForwarding <String> [-Delegates <PSListModifier>] [-DelegateRingWaitTime <TimeSpan>] [-SettingsActiveWorkHours]`

This cmdlet modifies the user's call forwarding settings.

- `Set-CsUserCallForwardingSettings [-Identity] <UserIdParameter> -EnableSimulRing <String> [-UnansweredToVoicemail] [-UnansweredWaitTime <TimeSpan>] [-Delegates <PSListModifier>] [-Team <PSListModifier>] [-TeamDelegateRingWaitTime <TimeSpan>] [-SettingsActiveWorkHours]`
- `Set-CsUserCallForwardingSettings [-Identity] <UserIdParameter> -EnableSimulRing <String> [-UnansweredToOther <String>] [-UnansweredWaitTime <TimeSpan>] [-Delegates <PSListModifier>] [-Team <PSListModifier>] [-TeamDelegateRingWaitTime <TimeSpan>] [-SettingsActiveWorkHours]`

This cmdlet modifies the SimulRing settings (again, with two parameter examples, one for unanswered to voicemail and the second being unanswered to other).

## Delegation settings

Administrators can change delegation settings by using the following cmdlet in PowerShell:

- `Get-CsuserDelegates -Identity <UserIdParameter>`

This cmdlet returns an object of delegates list, and displays the specified user's delegate list, in case of success. In case of failure, an appropriate error message will be shown.

- `Set-CsUserDelegates -Identity <UserIdParameter> [-Delegates <PSListModifier>]`

This cmdlet modifies the specified user's delegation settings, returns an object of delegates list and displays the list of delegates, in case of success. In case of failure, an appropriate error message will be shown.

- `Set-CsUserDelegates -Identity <UserIdParameter> [-Delegates @{add=[list]}] [-Delegates @{remove=[list]}]`

This cmdlet adds or removes a delegate.

- `Set-CsUserDelegates -Identity <UserIdParameter> [-Delegates @{replace=[list]}]`

This cmdlet sets a delegate list to specific delegates.

## Team members and related settings

Administrators can change team members and related settings by using the following cmdlet in PowerShell:

- `Get-CsUserTeamMembers -Identity <UserIdParameter>`

This cmdlet returns an object that contains list of team members, and displays the object on screen, in case of success. In case of failure, an appropriate error message will be shown.

- `Set-CsUserTeamMembers -Identity <UserIdParameter> [-Team <PSListModifier>]`

This cmdlet modifies the specified user's team members list, returns an object that contains the team member list and displays the object on the screen, in case of success. In case of failure, an appropriate error message will be shown.

- `Set-CsUserTeamMembers -Identity <UserIdParameter> [-Team @{add=[list]}] [-Team @{remove=[list]}]`

This cmdlet adds or removes team members.

- `Set-CsUserTeamMembers -Identity <UserIdParameter> [-Team @{replace=[list]}]`

This cmdlet sets a team list to specific members.

## More information

For on-premises deployments, the cmdlets introduced in this feature can only be run by members of the following groups, per the access level specified below:

- CsAdministrator – Get and Set for all cmdlets
- CsVoiceAdministrator - Get and Set for all cmdlets
- CsHelpDesk - Get for all cmdlets

For more information on these administrator roles, see [Create Skype for Business Server Control Panel Administrators](#). The administrator can access these cmdlets by directly or remotely logging on to a server computer. For a hybrid deployment, Skype for Business administrators should be able to call Get and Set for all cmdlets. For more information about the full list of roles, see [About Office 365 admin roles](#)

### NOTE

Server auto-discovery must be enabled. No additional licensing requirements will be introduced for use of the cmdlets.




# Skype for Business Server 2019 Management Tools



5/20/2019 • 2 minutes to read

**Summary:** Learn about the service management tools in Skype for Business Server 2019.

Skype for Business Server 2019 offers instant messaging (IM), presence, conferencing, and telephony solutions that support enterprise-level collaboration requirements. The tools to manage these services are both flexible and powerful.

## Skype for Business Server 2019 Tools

	CONTENT	DESCRIPTION
	<a href="#">Call Quality Dashboard</a>	The Call Quality Dashboard (CQD) is a web portal for quickly creating and organizing reports based on Quality of Experience (QoE) data from your Skype for Business environment. The CQD deploys a SSAS cube to aggregate the data in the QoEMetrics database, which enables users to create and modify reports and see them update in real-time. Additionally, CQD exposes web APIs that give users programmatic access to the cube data for use in custom dashboards.
	<a href="#">KHI Resources</a>	Key Health Indicators (KHI) are Performance Counters with recommended thresholds aimed at revealing problems that can impact the user experience. The KHI Guide outlines the operational process and remediation steps to maintain a healthy deployment, and includes a sample PowerShell script used to configure KHI Data Collectors and an Analysis and Definitions Workbook which can analyze KHI performance data.
	<a href="#">Statistics Manager for Skype for Business Server 2015</a>	StatsMan is a dashboard solution for viewing KHI calculations in real-time as well as graphed performance counters aggregated across your infrastructure. The dashboard can be used to pinpoint ongoing performance issues, view the results of a planned change to your environment, track resolution of outages, and much more. Out of the box, it is configured with KHI thresholds from the KHI Resources, and can be customized to suit your deployment's unique needs.

	<b>CONTENT</b>	<b>DESCRIPTION</b>
	<a href="#">Manage Skype for Business Server 2019 using SCOM Management pack</a>	<p>By using Skype for Business Server 2019 Management Packs, you can identify and address potential issues proactively. In this way, the Skype for Business Server 2019 Management Packs extend the capabilities of System Center Operations Manager.</p>
	<a href="#">Skype for Business Server Capacity Planning Calculator</a>	<p>The Skype for Business Server 2015/2019 Capacity Planning Calculator helps you model a topology for your organization's needs.</p>



# Call Quality Dashboard for Skype for Business Server

9/30/2019 • 2 minutes to read

**Summary:** Learn about the Call Quality Dashboard, which is a reporting tool for Skype for Business Server.

The Skype for Business Server Call Quality Dashboard (CQD) is a reporting layer on top of the Quality of Experience Database in the Monitoring Server in Skype for Business Server and Lync Server 2013. CQD uses Microsoft SQL Server Analysis Services to provide aggregate usage and call quality information as well as filtering and pivoting on the data set.

The following topics are included in this section and should be reviewed before deploying Call Quality Dashboard.

- [Plan for Call Quality Dashboard for Skype for Business Server](#)
- [Deploy Call Quality Dashboard for Skype for Business Server](#)
- [Use Call Quality Dashboard for Skype for Business Server](#)
- [Develop Call Quality Dashboard for Skype for Business Server](#)

# Plan for Call Quality Dashboard for Skype for Business Server

9/30/2019 • 20 minutes to read

**Summary:** Learn about what to consider when you plan for the Call Quality Dashboard.

## Overview of the Skype for Business Server Call Quality Dashboard

The Skype for Business Server Call Quality Dashboard (CQD) is a reporting layer on top of the Quality of Experience Database in the Monitoring Server in Skype for Business Server. CQD uses Microsoft SQL Server Analysis Services to provide aggregate usage and call quality information as well as for filtering and pivoting on the dataset. CQD features include:

- **Archival storage of QoE data via the QoE Archive component of CQD.** The QoE Archive component can store QoE data for a much longer duration than the Monitoring Server can. This allows for trending and reporting for up to seven months of data at a time, with the ability to slide the reporting window as far back as there is data.
- **Reporting and analysis using the power and speed of Microsoft SQL Server Analysis Services.** CQD utilizes Microsoft SQL Analysis Services to provide fast summary, filter, and pivoting capabilities to power the dashboard via an Analysis Cube. Reporting execution speed and the ability to drill down into the data can reduce analysis times dramatically.
- **New data schema optimized for call quality reporting.** The Cube has a schema designed for voice quality reporting and investigations. Portal users can focus on the reporting tasks instead of figuring out how the QoE Metrics database schema maps to the views they need. The combination of the QoE Archive and the Cube provides an abstraction that reduces the complexity of reporting and analysis via CQD. The QoE Archive database schema also contains tables that can be populated with deployment-specific data to enhance the overall value of the data.
- **Built-in report designer and in-place report editing.** The Portal component comes with several built-in reports modeled after the Call Quality Methodology. Portal users can modify the reports and create new reports via the Portal's editing functionality.
- **Web API access to the Report Structure and Analysis Cube Data.** The Dashboard reporting framework is not the only way to display the data from the Cube. CQD provides several examples of using HTML and JavaScript to retrieve data from the CQD Web APIs and render the data in a custom format. The combination of the Report Editor and the CQD Web APIs allows rapid prototyping of reports and custom report layout.

### NOTE

An admin can now manage Skype for Business Server 2019 using [CQD version 3](#) (log in with Admin credentials). This requires a hybrid implementation and the use of Call Data Connector (CDC). See [Plan Call Data Connector](#) for more information on enabling CDC. For CQD version 3 documentation, see [Turn on and use Call Quality Dashboard for Microsoft Teams and Skype for Business Online](#) for more information about CQD version 3.

## CQD Design Goals

CQD allows IT Pros to use aggregate data to identify focus areas in their environment experiencing media quality issues. It allows an IT Pro to compare statistics for different groups of users and identify trends and patterns. It is not focused on solving individual call issues, but on identifying problems and solutions that will apply to many users in a given environment.

# Call Quality Dashboard components

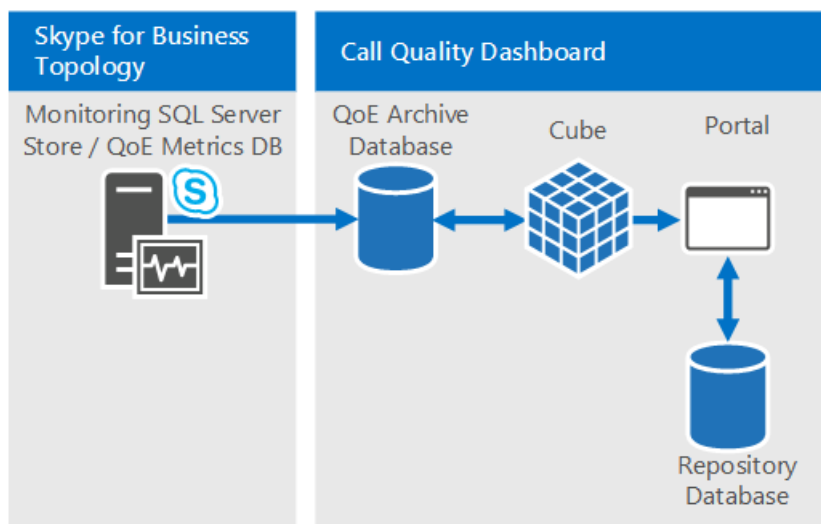
The Call Quality Dashboard consists of several databases, Microsoft SQL Agent jobs, processes, and web applications. The Microsoft SQL Agent jobs periodically copy data from the QoE Metrics database into the QoE Archive database and processes the Cube with the data in the QoE Archive database. The Repository database stores the report definitions that power the Portal. The Portal provides browser access to the Cube data.

The CQD components, including the QoE Archive, Cube, and Repository databases, can be installed on the Monitoring Server, installed on its own server, or installed across multiple servers. The particular installation method depends on the performance demands of CQD as well as impact to other processes on the same servers. For more information, refer to the "Components and topologies for CQD" section later in this article.

## Architectural Overview

To summarize, CQD requires the following elements:

- Two databases: an Archive Database and a Repository Database.
- One SSAS Cube visualizing aggregated data
- IIS hosts CQD Web Portal



The same CQD architecture supports Lync Server 2013 and Skype for Business.

## CQD and Skype for Business vs. Lync 2013

In a Skype for Business environment only, the following capabilities are available:

- Wi-Fi reporting of Signal Strength
- Wi-Fi reporting of Chipset drivers
- Rate my Call data

## Information available through CQD

CQD can show Skype for Business Server audio, video, and application sharing stream counts and count of good versus bad calls as well as ratios of bad to good calls. The views can be sliced and filtered by many different dimensions. CQD draws data from the QoE Metrics database in the Monitoring Server. The data is then merged with any customer-supplied data, such as network subnet-to-building mapping to make reports such as "Call Quality per Building" possible.

CQD also abstracts many of the internal QoE data idiosyncrasies such as "caller" and "callee" such that the user can focus on building report views around "server" and "client". Following the Call Quality Methodology, CQD is streamlined to help identify the conditions that pockets of poor calls have in common—one of the tenets for

improving call quality.

## Viewing data in CQD

The CQD data can be viewed via the CQD Portal and accessed via REST API calls.

### CQD Portal

The Portal is the fastest way to view the data in the Cube. The Portal comes with several built-in reports that are usable right away. The built-in reports are linked in a structured manner to guide the user to successively smaller and smaller slices of the call data. The built-in reports also highlight the various different ways the data can be shown by demonstrating a combination of charts and tables with different pivots, filters, and measures. Each user that accesses the Portal can have his or her own set of reports that he/she can modify and share. For more information on the usage of the CQD Web Portal, see [Use Call Quality Dashboard for Skype for Business Server](#).

Supported Operating Systems for CQD Portal: Windows 8.1, Windows 8, Windows Server 2012 R2, Windows Server 2012 , and Windows Server 2016 (Skype for Business Server 2019 CQD only).

Supported Browsers for CQD Portal: Internet Explorer 11, Internet Explorer 10, and Internet Explorer 9.

### REST APIs

The Cube data can also be accessed via REST API calls. The data retrieved via the REST API calls can be rendered via HTML pages. Users can take advantage of the query speed and the high level schema of CQD while still creating custom reports suited for their business needs. For more information on the API and samples, see [Develop Call Quality Dashboard for Skype for Business Server](#).

## Defining Your organization's requirements for CQD

CQD provides QoE data archiving and fast and deep analysis of call quality data. The following guide helps you to decide when and why you would deploy CQD.

### When to deploy CQD

**CQD can be deployed to establish a baseline call quality measurement, even if an organization doesn't experience call quality issues.** Establishing a baseline call quality measurement is important because every organization has a different mix of Wi-Fi versus wired and remote versus office workers. When call quality issues arise, the most recent call quality measurements can be compared to previous time intervals. CQD's trending features allow easy detection of changes in call quality over time.

**CQD can be deployed to proactively find problem areas that may impact call quality.** Even if the average call quality for an organization might meet the targets set by the organization, there could be pockets of call quality issues that are hidden behind average metrics. CQD allows pivot table-like breakdown of call quality metrics by many dimensions in the QoEMetrics database. Spotting outliers in peer groups is a quick way to proactively locate call quality issues.

**CQD should be deployed if there are call quality issues in the organization to reduce the time needed to troubleshoot problems.** CQD can simplify existing call quality investigations by offering fast reporting performance and dynamic drill down capabilities. CQD is designed for many kinds of workflows in call quality investigations validation of repairs to the environment.

### Why deploy CQD

**CQD should be deployed if QoE reporting needs to happen for more than 3 months of data.** The QoEMetrics database and monitoring server reports are designed to retain and report a small set of data. The QoE Metrics database is optimized for fast insertions, and therefore reporting performance can be impeded by large volume of calls or competing reporting access to the database. CQD's QoE Archive database provides a second copy of the QoE Metrics data with much longer retention capabilities. The Portal is also optimized to show up to 7 months of data at a time and can report on all the data in the QoE Archive as needed.

**CQD should be deployed if custom QoE reports are needed.** The Portal has a Report Editor feature for creating and prototyping reports quickly and easily. It also makes available REST APIs for programmatic access to the Cube data, allowing custom presentation using HTML/JavaScript or many other frameworks. It is no longer necessary to author new SQL queries for the purpose of creating custom data views for reporting.

**CQD should be deployed if existing QoE reporting functionality does not meet the speed or depth required by the organization.** CQD comes with many built-in reports. The reports are immediately useful and demonstrate how progressively drilling into the data can offer additional insights at each level. The reports hierarchy also helps with managing the numerous reports in a logical manner and fosters creation of many more reports that are easily accessible and understandable. CQD doesn't just offer speed and flexibility but also is optimized for the workflows developed by the Call Quality Methodology.

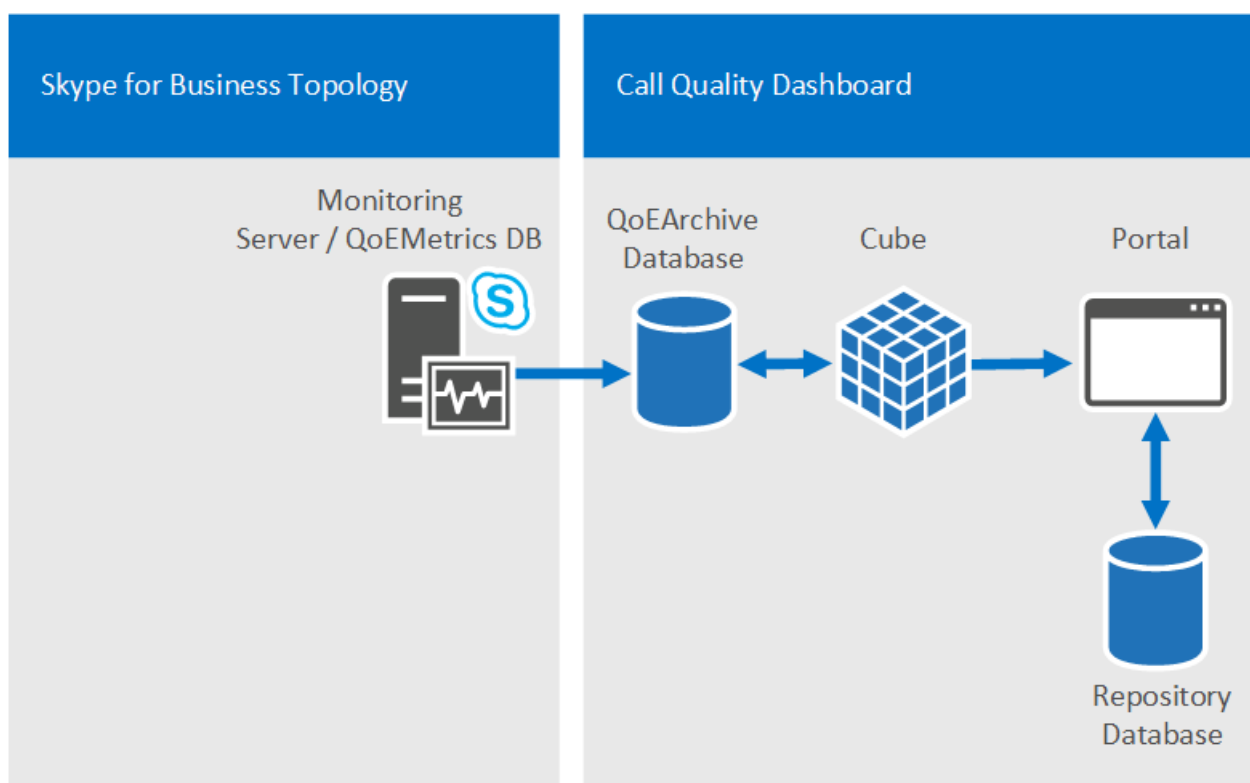
## Components and topologies for CQD

CQD comes with several components, and it helps to understand the requirements of each component and their relationship with each other to obtain the simplest and best performing deployment of the tool. The following table describes the dependent component for each CQD component.

COMPONENT NAME	DEPENDENT COMPONENT
QoE Archive	Microsoft SQL Server
Cube	Microsoft SQL Server Analysis Services
Portal	Microsoft Information Services
Repository Service (part of Portal installation)	Microsoft SQL Server

### NOTE

For QoE Archive and Cube, certain deployment options require Business Intelligence or Enterprise editions of Microsoft SQL Server. Refer to the [Infrastructure requirements for CQD](#) section below for more details.



## Single server configuration

All CQD components and dependent components can be installed onto one machine. The single box configuration is the simplest configuration and allows CQD to be self-contained. CQD would just need access to the QoE Metrics database on the Monitoring Server. The CQD Server can be a standalone machine, a virtual machine, or it can even be the Monitoring Server, depending on the available resources of the host machine and the performance requirements.

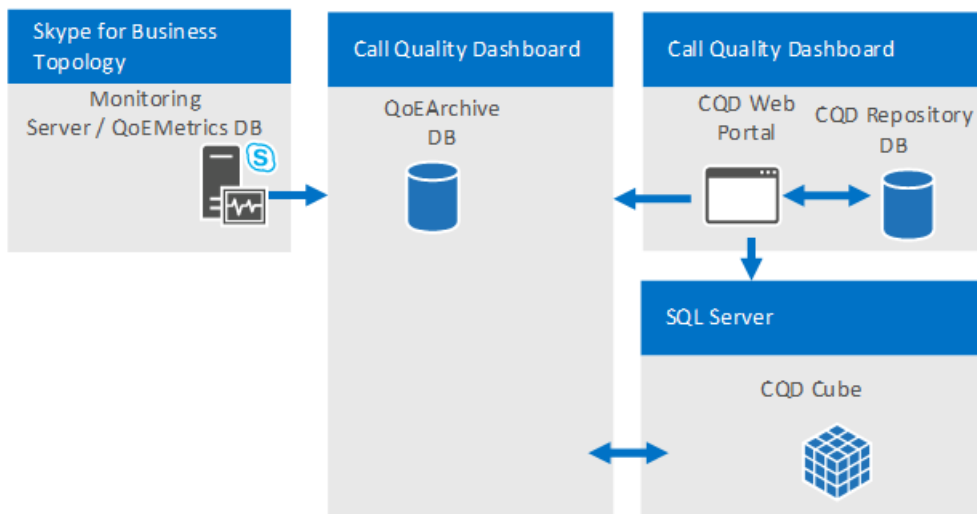
During installation, the user performing the installation simply needs to provide the Microsoft SQL Server and Microsoft SQL Server Analysis Services instances that have been previously set up on the machine where the CQD is to be installed. Please refer to [Deploy Call Quality Dashboard for Skype for Business Server](#) for more information.

## Multiserver configuration

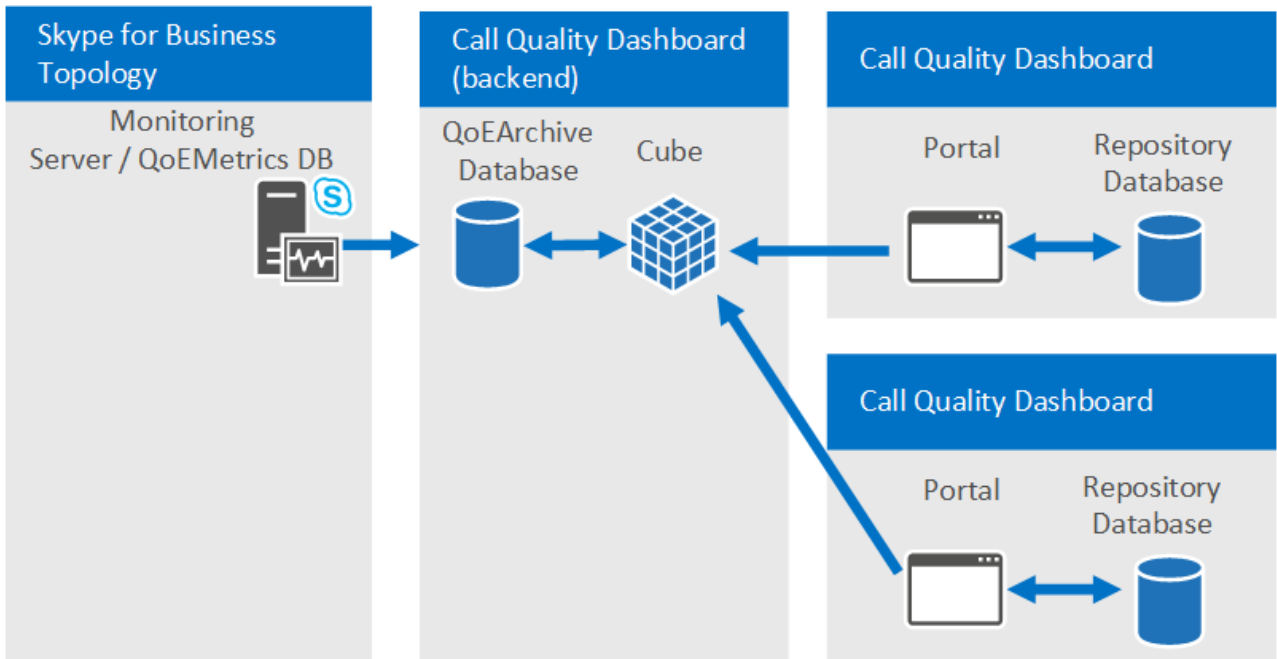
In a multiserver configuration, The QoE Archive, Cube, and Portal can all be on different machines. There are two main uses for the multiserver configuration:

- Hosting CQD Web Portal and CQD Cube on different servers.
- Hosting a "development" Portal separate from the "production" Portal.

**Hosting CQD Web Portal and CQD Cube on different machines.** Organizations that might have requirements to separate the CQD Portal from the SQL Server installation or that might want to mix and match SQL Server editions for the SQL Server instance and SQL Server Analysis Services instance can choose to install the CQD Portal and CQD Cube on different machines. The QoE Archive component can also be the sole CQD component that is installed if the organization simply wants to have a sustainable method to archive the QoE data without reaching performance limits on the Monitoring Server.



**Hosting a "development" Portal separate from the "production" Portal.** Organizations that develop their own custom reports (via the REST APIs) might prefer to deploy additional (CQD) Portal instances alongside the production Portal that regular users access for call quality monitoring or investigations. The development Portal can isolate any modifications to the Portal from the production environment. The additional web portals can be deployed on different machines (shown below) or deployed onto different web directories on the same machine (not shown). To accomplish the latter, the additional CQD web portal must be copied to the production machine manually because the CQD setup process always deploys the CQD Web Portal to the default web site with predefined web application names.



### Supported topologies

CQD does not merge data from multiple QoEMetrics databases, as is the case where there are multiple Skype for Business Server topologies, each with its own Monitoring Server. Each CQD instance must point to one QoEMetrics database. However, because CQD will move much of the reporting workload off of the Monitoring Server, large organizations that needed to deploy one Monitoring Server per Skype for Business Server topology should consider using one Monitoring Server for all topologies.

## Infrastructure requirements for CQD

CQD, including all its components and dependent components, can be deployed on a virtual machine, a single machine, or across multiple machines. The minimum software and hardware requirements are listed below. Data availability and query performance can vary from minutes to hours, depending on the number of active Skype for Business Server users and hardware and configuration, so some performance measurements are given below.

For CQD 2015	
Supported Operating Systems	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2
Supported SQL Server	SQL Server 2012, SQL Server 2014, SQL Server 2016
For CQD 2019	
Supported Operating Systems	Windows Server 2016, Windows Server 2019
Supported SQL Server	SQL Server 2017, SQL Server 2019

CQD utilizes Microsoft SQL Server, Microsoft SQL Server Analysis Services, and Microsoft Internet Information Services so CQD's minimum hardware and software requirements are basically the same as those dependent components. However, based on the organization's requirements around data freshness (which will depend in part on the volume of QoE data the organization generates) and deployment cost, additional deployment considerations should be made.

Data processing in CQD is separated into two main stages:

- QoE Archive process
- CQD Cube processing

**QoE Archive processing.** The QoE Archive processing task copies data from the QoE Metrics database on the Monitoring Server to the QoE Archive database. There are two situations where the processing time of the task would have fundamentally different performance characteristics. The first is after the initial installation of CQD. When the task is run for the first time after a fresh installation, the QoE Archive processing task will copy all the data that is in the QoE Metrics database into QoE Archive database. The second is the periodic processing after this initial round. The QoE Archive processing task will run every 15 minutes and process any new QoE records that are in the QoE Metrics database. Generally, the initial processing time is not a concern because it is run only the first time, when CQD is installed. However, if the CQD server is severely under-provisioned, this task can take several hours. Refer to the table below for example initial QoE Archive processing times.

**CQD Cube processing.** The Cube processing task aggregates the data from the QoE Archive database into the Cube. The initial cube processing time and subsequent cube processing time are determined by the SQL Server Analysis Services edition used for the CQD Cube. If the Standard edition is used, there is no difference between the initial cube processing time and the subsequent cube processing time because each time the Cube data is refreshed, it will always be a full processing of all available data. (This means that the Cube processing time increases as the amount of data in the QoE Archive database increases.) Because the Business Intelligence Edition and Enterprise Edition of SQL Server have partition support, if either edition is used, only the initial run will process all data in the QoE Archive database. In subsequent runs, when the task is triggered every 15 minutes, the task will only process the new records added to the QoE Archive database since the last time the task was run. Once a day, there will also be a full processing on the partition that contains the current month's data.

The physical machine characteristics can affect CQD performance as well as the software features that are available from the SQL Server components. The QoE Archive component will be more disk-intensive compared to other components, whereas the Cube component will be more CPU and memory intensive. All of these factors contribute to CQD's total data processing time, which directly affects data freshness and availability. Organizations should make decisions on the hardware and software based on the individual needs of the organization.

### Tested Hardware Configurations

This section makes the assumption that there is a single QoEMetrics DB in the environment.

#### Machine profiles

MACHINE	CPU CORES	RAM	QOE ARCHIVE AND CUBE ON SAME DISK	QOE ARCHIVE AND SQL TEMP DB ON SAME DISK
Virtual machine	4	7 GB	Yes	Yes
4 core	4	20 GB	Yes	No
8 core	8	32 GB	Yes	No
16 core	16	128 GB	No	No

#### Performance results



MACHINE	QOE METRICS DB SIZE	SQL PARTITIONS	DISK TYPE	NUMBER OF STREAMS	INITIAL ARCHIVE PROCESS	INITIAL CUBE PROCESS	SUBSEQUENT ARCHIVE PROCESS	SUBSEQUENT CUBE PROCESS
Virtual machine	900 MB	Single	VHD (variable-size)	.5 M	30 m	2 m	30 s	1 m
Virtual machine	9 GB	Single	VHD (variable-size)	5 M	4 h	15 m	1 m	5 m
Virtual machine	9 GB	Single	VHD (fixed-size)	5 M	2 h	5 m	1 m	5 m
Virtual machine	30+ GB	Single	VHD (fixed-size)	10 M	15 h	20 m	2 m	45 m
8 core	9 GB	Single	Multiple Disks	5 M	2 h	5 m	25 s	5 m
8 core	9 GB	Multiple	Multiple Disks	5 M	2 h	15 m	35 s	2 m
8 core	30+ GB	Single	Multiple Disks	20 M	9 h	20 m	1 m	20 m
8 core	30+ GB	Multiple	Multiple Disks	20 M	9 h	30 m	2 m	2 m
4 core	200 GB	Single	Multiple Disks	125 M	6+ days	7 h	2 m	6 h
16 core	500 GB	Multiple	Multiple Spindles	250 M	8 days	2 h	2 m	10 m

\*These are not expected to be encountered in real deployments because the QoE Metrics database would have to have 9 and 18 months of data, respectively, but they're provided here for completeness.

### Service Account Requirements

You will need an account (with read access to QoEMetrics) that the SQL Agent on the CQD Server can use for importing data to the QoEArchiveDB.

You may also need to configure a separate account for an SSAS Job to pull data from QoEArchiveDB (this is an optional process).

IIS most commonly uses Network Service as App Pool Identity, but can be configured to a Service Account.

### Portal Access Control

By default, any authenticated user has access. This can be changed by using IIS Authorization rules to restrict to a specific group.

### Pre-Install Requirements

These instructions assume that a QoE Metrics database has already been installed and is running somewhere in the Skype for Business Server topology.

## Hardware Requirements

CQD utilizes Microsoft SQL Server, Microsoft SQL Analysis Server, and Microsoft Internet Information Server so CQD's minimum hardware and software requirements are basically the same as those dependent components. However, based on the organization's requirements around data freshness (which will depend in part on the volume of QoE data the organization generates) and deployment cost, additional deployment considerations should be made.

## Software Requirements

The following operating systems are required for CQD:

- Windows Server 2008 R2 with IIS 7.5
- Windows Server 2012 with IIS 8.0
- Windows Server 2012 R2 with IIS 8.5
- Windows Server 2016 with IIS 10.0 (Skype for Business Server 2019 CQD only)
- Windows Server 2019 (Skype for Business Server 2019 CQD only)

The following are the required IIS role services (in hierarchical order):

- Web Server
  - Common HTTP Features
  - Static Content
  - Default Document
  - Application Development
  - ASP.NET
  - ISAPI Filters
  - Health & Diagnostics
  - HTTP Logging
  - Security
  - URL Authorization
  - Windows Authentication
  - Management Tools
  - IIS Management Console

### NOTE

Note the following for the above requirements:> 3.5 and 4.5 versions of the .Net framework are available. Both are required (more specifically, 3.5 SP1 is required).> In some systems, if ASP.NET is setup before IIS install, then ASP.NET may not be registered in IIS. The problem manifests through the absence of application pools for the corresponding .Net version and also missing the .NET CLR version in app pool configuration. To correct such an issue on Windows Server 2008 R2, execute `%systemroot%\Microsoft.NET\Framework64\4.0.30319\aspnet_regiis.exe -iru`. On Windows Server 2012 and Windows Server 2012 R2, execute `dism /online /enable-Feature /all /FeatureName:WCF-HTTP-Activation45` followed by removing the "ServiceModel" module from the Default Web Site in IIS Manager.> Management tools is optional, but recommended.

To install these requirements using PowerShell, run the following:

```
import-module servermanager
```

```
add-windowsfeature Web-Server, Web-Static-Content, Web-Default-Doc, Web-Asp-Net, Web-Asp-Net45, Web-Net-Ext, Web-Net-Ext45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Url-Auth, Web-Windows-Auth, Web-Mgmt-Console
```

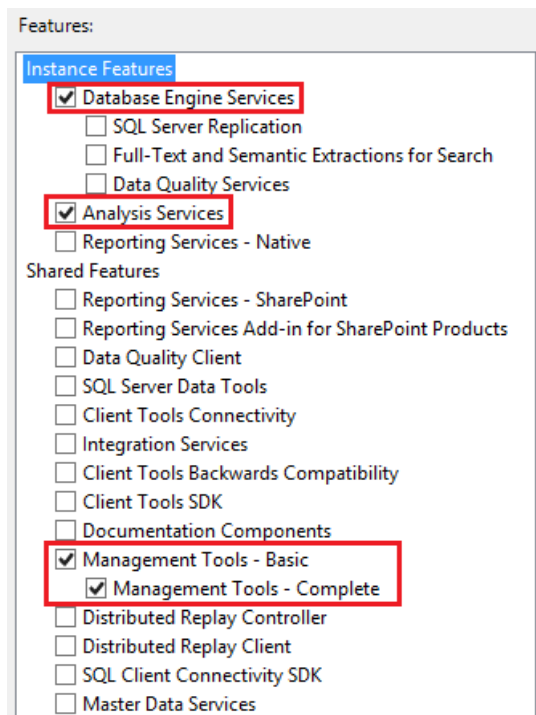
The following versions of SQL Server are supported:

- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019 (Skype for Business Server 2019 CQD only)

Business Intelligence or Enterprise edition is recommended for performance reasons. These editions allow use of multiple partition files that can be processed in parallel, which is beneficial for processing data spanning multiple months or longer.

While not recommended, Standard edition is supported as well. Processing will be constrained to a single partition (which needs to be configured during setup).

In all cases, "Database Engine Services" and "Analysis Services" must be installed. It is recommended but not required to also install the "Management Tools - Complete" feature, which adds SQL Server Management Studio support for Analysis Services. Feature selection screen should look like the figure.



When configuring the SSAS setup, in the Analysis Services Configuration, set "Server Mode" to "Multidimensional and Data Mining Mode".

For additional help in installing and configuring SQL Server Business Intelligence Features, see [Install Analysis Services in Multidimensional and Data Mining Mode](#).

#### Account Requirements

Three domain service accounts are recommended on the principle of least privilege:

- One that already has both a login security principal for QoE Metrics database (with db\_datareader privilege) and a login security principal in QoE Archive SQL Server Instance (needed to create a Linked Server object during setup). This account will be used to run "QoE Archive Data" step of the SQL Server Agent job.
- One that will be used to run "Process Cube" step of the SQL Server Agent job. Setup will create a login security principal to QoE Archive database (with read and write privilege) and also create a member in the QoE Role (with full control privilege) for the Cube.
- One that will be used to run IIS Worker Process for the web portals and web APIs. Setup will create a login security principal to QoE Archive database (with read privilege), a login security principal to Repository database (with read and write privilege) , and a member in QoERole (with full control privilege) for the Cube.

**NOTE**

When both QoE Archive database and Repository database are hosted in the same SQL Server, only one login security principal with two user mappings is created.

The first two accounts can be logically considered as "back end service accounts" and the last account is a "front end service account". While not recommended, it is possible to use a single account in all cases.

**NOTE**

The user account initiating the installation must have read access to QoE Metrics DB as well (in addition to having machine admin rights on the QoE Archive DB server where the installation must take place).

## Capacity Planning

CQD is designed for minimal Impact on QoEMetrics: the code has been optimized to not lock data, and import jobs are tunable.

The type of hardware to use depends on your requirements for how quickly syncs should run. Disk Sizing is as follows:

- QoEArchive is ~1.5x larger than QoEMetrics DB initially
- SSIS Cube compresses the data almost 10x compared to DB
- Data is partitioned monthly; partitions can be deleted

# Deploy Call Quality Dashboard for Skype for Business Server

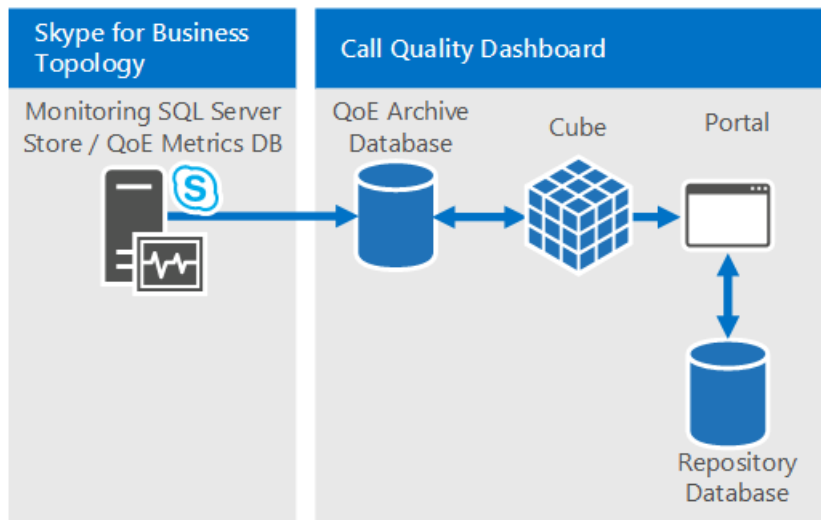
6/25/2019 • 16 minutes to read

**Summary:** Learn about the deployment process for Call Quality Dashboard. Call Quality Dashboard is a tool for Skype for Business Server.

## Deployment Overview

Call Quality Dashboard (CQD) consists of three major components:

- **Archive Database**, where the Quality of Experience (QoE) data is replicated and stored.
- **Cube**, where data from QoE Archive database is aggregated for optimized and fast access.
- **Portal**, where users can easily query and visualize QoE data.



The setup process for QoE Archive involves creating the QoE Archive database, deploying a SQL Server stored procedure that will move the data from the source QoE Metrics database into QoE Archive database, and setting up the SQL Server Agent job to execute the stored procedure at a regular interval.

Cube deployment gets information from the user on where the QoE Archive is located, deploys the cube, and sets up a regular SQL Server agent job that will refresh the cube at a regular interval.

Portal install creates a Repository database that stores the mapping of CQD users to each user's reports/queries. It then sets up an IIS web application which is the dashboard where users can see a pre-defined set of reports as well as customize and create their own queries to visualize data from the cube. The portal install creates two additional web applications that exposes APIs for users to programmatically access the repository and the cube. (These APIs are used internally by the dashboard as well.)

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
Install prerequisite hardware and software.	Decide on the CQD configuration, and choose a SQL Server from which to perform the install.	Domain user who is a member of the local administrators group.	"Pre-install Requirements" section in the deployment documentation.

PHASE	STEPS	ROLES AND GROUP MEMBERSHIP	DOCUMENTATION
Install CQD.	Run the MSI following the deployment document.	To perform the setup, the installing account must be a domain user who is a member of the local administrators group and have read access to QoE Metrics database on the Monitoring Server.	"Accounts and Deployment Steps" sections in the deployment documentation.
Grant user access.	For managing user authorization to the Portal, we recommend using URL Authorization, which was introduced in IIS 7.0. For more information, see <a href="#">Understanding IIS 7.0 URL Authorization</a> .	Domain user who is a member of the local administrators group.	Managing User Access for the Portal section in the deployment documentation.
Optional: Provide subnet mapping information.	Populate network and building mapping tables in QoE Archive database.	An account with write access to the QoE Archive database.	"Supplying Subnet Information" section in the user documentation.

Deployment of Call Quality Dashboard involves setting up the infrastructure and installing the software. The following procedure outlines the process.

## Deployment Steps

1. Copy the CallQualityDashboard.msi to the machine where the archive database component of CQD is to be installed (this is the machine that has SQL Server installed).
2. Execute the MSI (Windows will prompt to run with administrator privilege, do so).
3. Accept the EULA.
4. Select the destination folder where files related to Call Quality Dashboard components will be located or accept the default location.
5. Select all features.
6. At the QoE Archive Configuration page, provide the following information:
  - **QoE Metrics SQL Server:** SQL Server instance name for where the QoE Metrics DB is located (this will be the data source).
  - **QoE Archive SQL Server Name:** This is read-only field and fixed to the fully qualified domain name of the local machine. Archive DB can be installed only on the local machine.
  - **QoE Archive SQL Server Instance:** A local SQL Server instance name for where the Archive DB is to be created. To use a default SQL Server instance, leave this field blank. To use a named SQL Server instance, specify the instance name (e.g. the name after the "").
  - **QoE Archive Database:** By default, this option is set to "Create new database". Since Archive DB upgrade is not supported, the only circumstance under which the "Use existing database" option can be used is if the existing Archive database has the same schema as the build to be installed.
  - **Database File Directory:** Path to where the database files (.mdf and .ldf) for the Archive DB should be placed. This should be on a drive (HDD2 in the recommended hardware configuration) separate

from the OS. Note that since the file names are fixed in the install, to avoid any potential conflict, it is recommended that a blank directory with no files be used.

- **Use Multiple Partitions:** The default is set to "Multiple partition", which requires Business Intelligence edition or Enterprise edition of SQL Server. For Standard edition, select "Single Partition" option. Note that cube processing performance may be impacted if Single Partition is used.

#### NOTE

The selection for Use Multiple Partitions option cannot be changed once Setup completes. In order to change it, the Cube feature needs to be first uninstalled and then reinstalled using "Change" option in Control Panel.

- **Partition File Directory:** Path to where the partitions for the QoE Archive database should be placed. This should be on a drive (HDD3 in the recommended hardware configuration) separate from the OS drive and SQL database log files drive. Note that since the file names are fixed in the install, to avoid any potential conflict, it is recommended that a blank directory with no files be used.
- **SQL Agent Job User - User Name & Password:** Domain service account name and password (masked) that will be used to run the "QoE Archive Data" step of the SQL Server Agent job (which will run the stored procedure to fetch data from QoE Metrics DB into Archive DB, so this account must have read access to QoE Metrics DB, as indicated under Accounts section. This account also needs to have a login in the QoE Archive SQL Server Instance).

#### NOTE

The account that the SQL Server instance is running under, such as NT SERVICE\MSSQLSERVER, must have access/permission to the directories given above for the installation to succeed. For details, see [Configure File System Permissions for Database Engine Access](#)

7. Upon clicking next, the installer will perform pre-requisite checks and report if any issues are encountered. When all pre-requisite checks pass, the installer will go to the Cube Configuration page.

#### NOTE

If the installer shows a warning message that the SQL Server Agent service for the QoE Archive SQL Server instance is currently not running, installation can proceed, but post installation please make sure that SQL Agent service is running and set the Startup type to Automatic so that the scheduled Job runs.

8. At Cube Configuration page, provide the following information:

- **QoE Archive SQL Server Name:** This is read-only field and fixed to the fully qualified domain name of the local machine. Cube can be installed only from the machine that has QoE Archive database (Note. Cube itself may be installed on a remote machine. See below)
- **QoE Archive SQL Server Instance:** SQL Server instance name for where the QoE Archive DB is located. To specify a default SQL Server instance, leave this field blank. To specify a named SQL Server instance, enter the instance name (e.g. the name after the ""). If QoE Archive component was selected for the install, this field will be pre-populated with the value provided on the QoE Archive Configuration page.
- **Cube Analysis Server:** SQL Server Analysis Service instance name for where the cube is to be created. This can be a different machine but the installing user has to be a member of Server administrators of the target SQL Server Analysis Service instance.

**NOTE**

For more information about configuring Analysis Services Server Administrator Permissions, see [Grant Server Administrator Permissions \(Analysis Services\)](#)

- **Use Multiple Partitions:** The default is set to "Multiple partition", which requires Business Intelligence edition or Enterprise edition of SQL Server. For Standard edition, select "Single Partition" option. Note that cube processing performance may be impacted if Single Partition is used

**NOTE**

The selection for Use Multiple Partitions option cannot be changed once Setup completes. In order to change it, the Cube feature needs to be first uninstalled and then reinstalled using "Change" option in Control Panel.

- **Cube User - User Name & Password:** Domain service account name and password (masked) that will trigger the cube processing. If QoE Archive component was selected for the install, this field will be pre-populated with the value provided on the Archive Configuration page for the SQL Agent Job User, but we recommend specifying a different domain service account so that Setup can grant the least required privilege to it.
9. When clicking next, another round of validation will be performed and any issue will be reported. Upon successful completion of the validation, the installer will go to the Portal Configuration page.
  10. At Portal Configuration page, provide the following information:
    - **QoE Archive SQL Server:** SQL Server instance name for where the QoE Archive database is located. Note that unlike the QoE Archive Configuration page and the Cube Configuration page, the machine name is not fixed and must be provided. If QoE Archive component was selected for the install, this field will be pre-populated with the value provided on the QoE Archive Configuration page.
    - **Cube Analysis Server:** SQL Server Analysis Service instance name for where the cube is located. If Cube component was selected for the install, this field will be pre-populated with the value provided on the Cube Configuration page.
    - **Repository SQL Server:** SQL Server instance name where the Repository database is to be created. If the SQL Server instance name for where the QoE Archive database is located has been provided earlier in the setup (in other components), this field will be pre-populated with the QoE Archive DB SQL Server instance name. This can be any SQL Server instance.
    - **Repository Database:** By default the option is set to "Create new database". Since Repository DB upgrade is not supported, the only circumstance under which the "Use existing database" option can be used is if the existing Repository DB has the same schema as the build to be installed.
    - **IIS App Pool User - User Name & Password:** The account that the IIS application pool should execute under. The User Name and Password fields will be grayed out if built-in system accounts are selected. These fields will only be enabled if "Other" is selected from the drop down box so the user can enter the domain service account information.
  11. When clicking next, the final round of validation will be done to ensure that the SQL Server instances are accessible using the credentials provided and that IIS is available on the machine. Upon successful completion of the validation, the installer will proceed with the setup.

When the installer is done, most likely the SQL Server Agent job will be in progress, doing the initial load of the



QoE data and the cube processing. Depending on the amount of data in QoE, the portal will not have data available for viewing yet. To check on the status of the data load and cube processing, go to

<http://<machinename>/CQD/#/Health>.

#### NOTE

Note that the URL for checking the status of the download cube processing is case sensitive. If you enter 'health' the URL will not work. You must enter 'Health' at the end of the URL with a capital H.

Detailed log messages will be shown if debug mode is enabled. To enable debug mode, go to **%SYSTEMDRIVE%\Program Files\Skype For Business 2015 CQD\QoEDataService\web.config**, and update the following line so the value is set to **True**:

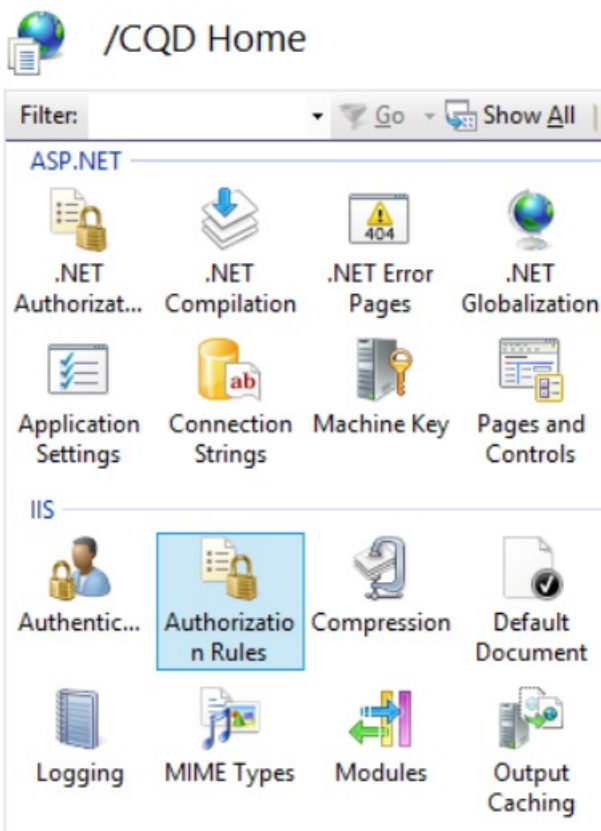
```
<add key="QoEDataLib.DebugMode" value="True" />
```

The main portal page is accessible via <http://<machinename>/CQD>.

## Managing User Access for the Portal

For managing user authorization to the Portal, we recommend using URL Authorization, which was introduced in IIS 7.0. For more information on IIS security, see [Understanding IIS 7.0 URL Authorization](#).

Any web site or web application inherit the default URL Authorization configured for the entire IIS, which is typically "Allow All Users". If access to the Portal needs to be more restrictive, then administrators can grant access to only the specific group of users by editing the "Authorization Rules".



#### NOTE

The Authorization Rules icon is not to be confused with the ".NET Authorization" under the ASP.NET section, which is a different authorization mechanism.

Administrators should first remove the inherited "Allow All Users" rule. This prevents any non-authorized users from accessing the Portal.



## Authorization Rules

Use this feature to specify rules for authorizing users to access websites and applications.

Mode	Users	Roles	Verbs	Entry Type
Allow	All Users			Inherited

Next, administrators should add new Allow Rules and give specific users the permission to access the Portal. It is recommended that a local Group called "CQDPortalUsers" be created to manage the users.



## Authorization Rules

Use this feature to specify rules for authorizing users to access websites and applications.

Mode	Users	Roles	Verbs	Entry Type
Allow		CQDPortalUsers		Local

The configuration details are stored in the web.config located at the Portal's physical directory.

```
<?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <security> <authorization> <remove users="*" roles="" verbs="" /> <add accessType="Allow" roles="CQDPortalUsers" /> </authorization> </security> </system.webServer> </configuration>
```

The next step is to configure the dashboard of the CQD. After users are authenticated by IIS, they will have to have file permissions on the CQD directory in order to access the web portal content. It is possible to change the ACLs through the security tab of the CQD directory properties to add individual users or groups; however the recommended approach is to leave the file permissions untouched. Instead, change the IIS setting to use the IIS worker process to access the CQD directory no matter which user is authenticated.

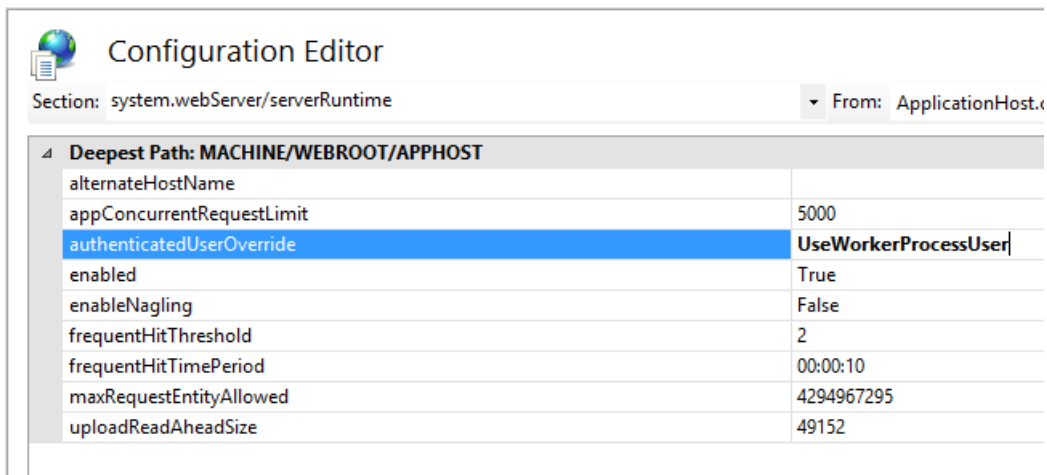
### IMPORTANT

It is important to only change this setting for the CQD application, and not for the two API applications: QoEDataService and QoERepositoryService.

## Configuring File Access for the CQD (Dashboard)

1. Open the Configuration Editor for CQD.





4. Click **Apply** on the right-hand side of the page.

## Known Issues

### The CQD shows no data after deployment

You may receive the following error:

*We couldn't perform the query while running it on the Cube. Use the Query Editor to modify the query and fix any issues. Also make sure that the Cube is accessible.*

This means that the cube must be processed in SQL Server Analysis Services prior to being used in CQD. You can resolve this by following these steps:

1. Open SQL Management Studio and select **Analysis Services**.
2. Expand the **QoECube** object, select **QoE Metric**, right-click, and then choose **Browse**.

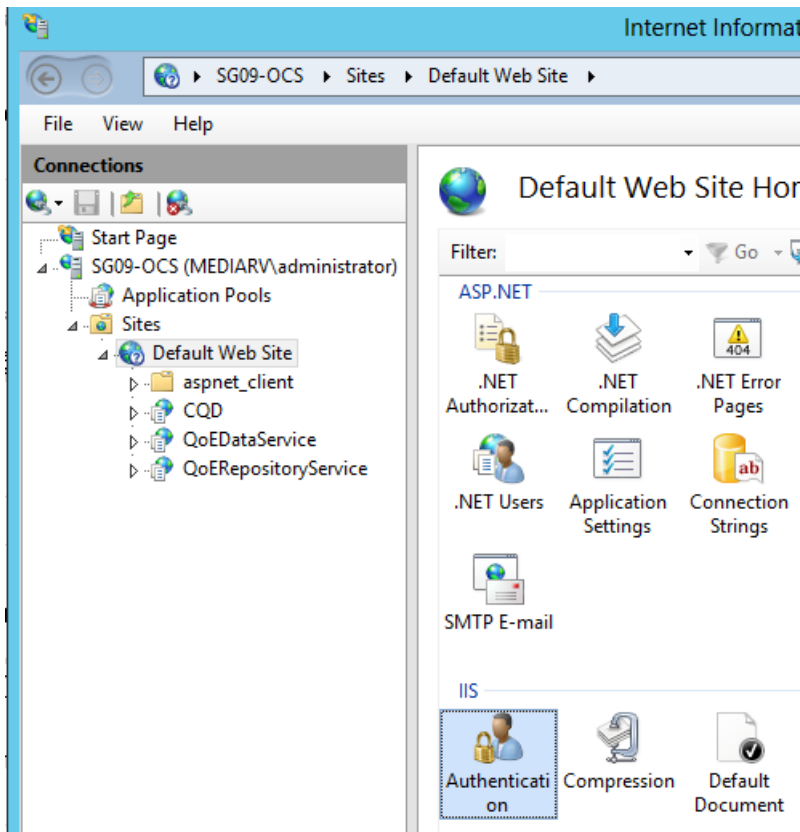
If this returns empty browser, the cube hasn't been processed yet.

3. Right-click **QoE Metric** again and choose **Process**.
4. When processing is complete, right-click the object again, and choose **Browse** to confirm that the browser page now shows data.

### Users have trouble logging in because installer fails to create the correct settings in IIS

In rare cases, the installer fails to create the correct settings in IIS. Manual change is required to allow users to log into the CQD. If users are having trouble logging in, please follow these steps:

1. Open up IIS Manager, and navigate to Default Web Site.



- Click on "Authentication". If the "Anonymous Authentication", "ASP.NET Impersonation", "Form Authentication", and "Windows Authentication" do not match the settings shown below, manually change them to match the settings below. All other authentication mechanisms should be disabled.

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

- For "Windows Authentication", click on Advanced Settings on the right-hand side.

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

**Alerts**

[Click here to learn how to configure Extended Protection.](#)

**Actions**

[Disable](#)

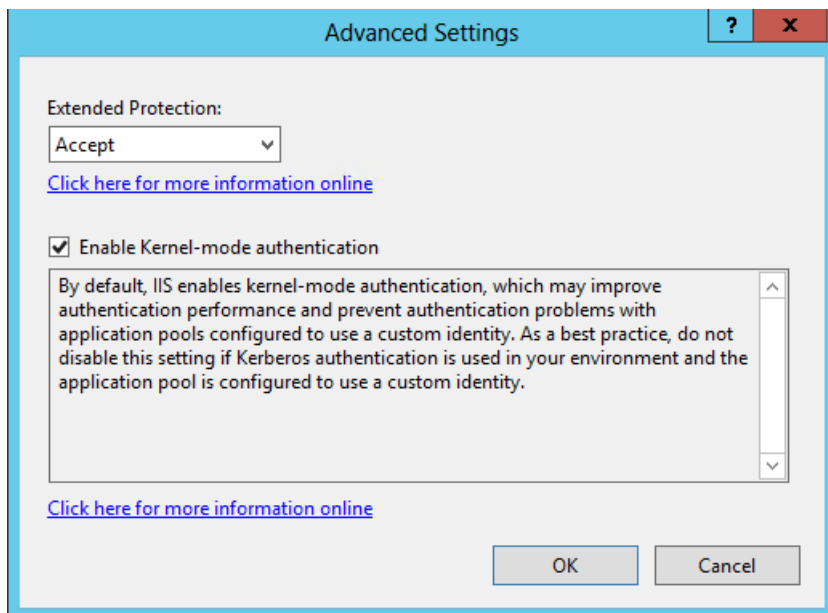
[Advanced Settings...](#)

[Providers...](#)

[Help](#)

[Online Help](#)

- Set "Extended Protection" to Accept and check the "Enable Kernel-mode authentication" box.



5. Repeat the above steps for each of the "CQD", "QoEDataService", and "QoERepositoryService" entries below "Default Web Site".

For HTTP and HTTPS port bindings the installer will create port bindings on the default port numbers (port 80 for HTTP and port 443 for HTTPS). If there is another website on the machine that uses these bindings, there will be a conflict and the IIS behavior cannot be predicted. The best way to avoid this problem is to make sure that no other websites are mapped to ports 80 and 443 before installing CQD.

To enable SSL/TLS in IIS and force users to connect via secure HTTPS instead of HTTP:

1. Configure Secure Sockets Layer in IIS, see [Configuring Secure Sockets Layer in IIS 7](#). Once done, replace `http` with `https`.
2. For instructions on enabling TLS in the SQL Server connections, see [How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console](#).

## Cube Sync Fails

QoEMetrics may contain some invalid records based on end user clocks. If the time skew is greater than 60 yrs, the cube import will fail.

Check the Min and Max StartTime/EndTime using the selections below. Look for and delete records in the far past and very distant future, they can be disregarded and they will break up the sync processes.

- Select MIN(StartTime) FROM CqdPartitionedStreamView
- Select MAX(StartTime) FROM CqdPartitionedStreamView
- Select MIN(EndTime) FROM CqdPartitionedStreamView
- Select MAX(EndTime) FROM CqdPartitionedStreamView

## Post-install tasks

### Importing Buildings and Networks

After Installing CQD, perform the following configuration tasks:

1. Define Building types (recommended)
2. Define Building Ownership types (recommended)

3. Define Network types (highly recommended)
4. Import Buildings (recommended)
5. Import Subnets (recommended)

### Define Building Types

Building types are used to describe the different buildings definitions or types within your organization.

#### NOTE

This step is optional, but recommended.

#### Examples

- Headquarters
- Remote Office
- Joint-venture location

#### Sample SQL Syntax

```
INSERT INTO
[dbo].[CqdBuildingType]
([BuildingTypeId],
[BuildingTypeDesc])
VALUES
(1,
'Headquarters')
```

The BuildingTypeId and BuildingTypeDesc parameters are required.

### Define Building Ownership Types

Ownership types are used to distinguish owned vs leased assets.

#### NOTE

This step is optional, but recommended.

#### Examples

- Contoso Leased non-RE&F
- Contoso Leased RE&F
- Contoso Owned
- Subsidiary Leased

#### Sample SQL Syntax

```
INSERT INTO
[dbo].[CqdBuildingOwnershipType]
([OwnershipTypeId],
[OwnershipTypeDesc]
)

VALUES
(1,
'Contoso Owned'
)
```

The OwnershipTypeId and OwnershipTypeDesc parameters are required.

### Define Network Names

Network Types are used to describe different types of networks within the organization. This gives you the ability to filter on (or filter out) specific Network Types.

#### NOTE

It is highly recommended to define Network Names, but it is optional. If you decide to not define network names, ensure the each CqdNetwork entry has a BuildingId of 0.

#### Examples

- VPN
- LAB

#### Sample SQL Syntax

```
INSERT INTO [dbo].[CqdNetworkName]
( [NetworkName]
,[NetworkType]
)
VALUES
('VPN', 'VPN')
```

The NetworkNameID and NetworkName parameters are required, the NetworkType parameter is optional but recommended.

### Import Buildings

Importing Buildings gives you the ability to get building specific insights (poor calls per building on WiFi/Wired, etc.).

#### NOTE

This step is optional, but recommended.

Before you Import a new building you should already have a predefined BuildingKey identified. To do that, issue the "SELECT MAX(BuildingKey) FROM CqdBuilding" SQL command to identify the current value and add 1 to the result.

#### Sample SQL Syntax



```
INSERT INTO [dbo].[CqdBuilding]
( [BuildingKey]
,[BuildingName]
,[BuildingShortName]
,[OwnershipTypeId],
[BuildingTypeId]
)
VALUES
(2, 'Ann Arbor', 'AA', 0, 0)
```

The BuildingKey, BuildingName, BuildingShortName, OwnershipTypeId, BuildingTypeId parameters are required, the other parameters are optional.

### Import Subnets

Importing Buildings gives you the ability to get building specific insights (poor calls per building on WiFi/Wired, etc.).

#### NOTE

This step is optional, but recommended.

Import Subnets and map them to the Buildings imported in the last step. If you decided not to populate NetworkName, ensure each entry in this table uses a NetworkNameID of 0.

### Sample SQL Syntax

```
INSERT INTO [dbo].[CqdNetwork]
([Network]
,[NetworkNameID]
,[BuildingKey]
,[UpdatedDate]
)
VALUES
('172.16.254.0',0,1,'2015-11-11')
```

The Network, and UpdatedDate parameters are required, the other parameters are optional.

### Optional: BSSID

Populating BSSID information gives you additional WiFi stream correlation by controller or radio. This is in addition to filtering by building or subnet.

### Sample SQL Syntax

```
INSERT INTO [dbo].[CqdBssid]
([Ap],
[Bss],
[Building],
[ess],
[phy]
)
VALUES
('AP1','00-00-00-00-00-00','Aruba AP 1','Controller1','bgn')
```

### CqdBssidTable Details

AS SHOWN IN CQD	CQDBSSID TABLE	EXAMPLE INPUTS
Ap NName	AP	AP1
BBssid	BSS	00-00-00-00-00-00 (you must use the delimited fformat)
Controller	Building	Aruba AP 7
Device	ess	Controller1
Radio	phy	bgn

### Processing the imported data

By default, after you import building/network data it will only apply to records generated after that point in time.

To tag all the previous records with this new data, you will need to run the CqdUpdateBuilding stored procedure as shown below:

Give it the date of your first record (identify that using the `Select MIN(StartTime) FROM CqdPartitionedStreamView` SQL command ), an EndDate of tomorrow, then NULL for the last two values.

Once the data is associated with stream data, the SSIS Cube needs to reprocess all records. This also applies when bulk adding BSSID/ISP data. Ensure that "Process Full" is selected.

# Use Call Quality Dashboard for Skype for Business Server

9/6/2019 • 9 minutes to read

**Summary:** Learn about how to use the Call Quality Dashboard. Call Quality Dashboard is a tool for Skype for Business Server.

Call Quality Dashboard (CQD) allows IT Pros to use aggregate data to identify problems creating media quality issues by comparing statistics for groups of users to identify trends and patterns. CQD is not focused on solving individual call issues, but on identifying problems and solutions that apply to many users.

## Call Quality Dashboard User Guide

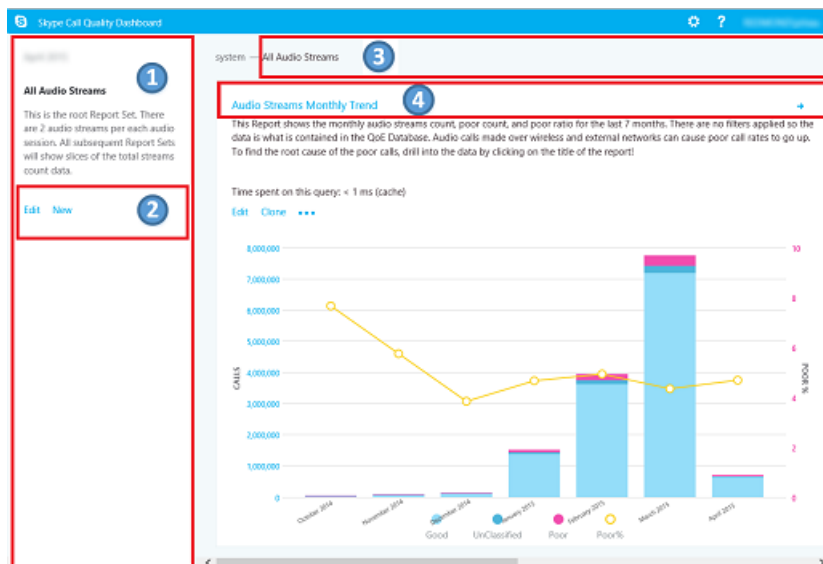
CQD is a web portal for quickly creating and organizing reports based on Quality of Experience (QoE) data. CQD deploys an SSAS cube to aggregate the data in the QoE Metrics database, and enables admins to create and modify reports or do investigations in real time. While it is possible to use Excel to connect directly to the cube, the portal is optimized for several workflows involving QoE data. The data includes:

- Cached report data for fast access
- Deep links to report pages for information sharing and publishing
- Streamlined report editing and creation, and editable metadata for report descriptions.

Also, CQD exposes web APIs that give users programmatic access to the cube data for use in custom dashboards.

### Feature Overview

When you visit the Call Quality Dashboard, you see the following screen:



1. The "Summary Pane" is where context for the "Report Set" (to the right) can be found.
2. Click "Edit" in the Summary Pane Report to set level properties (including Y-axis height).
3. The Breadcrumb helps you identify your current location within the report set hierarchy.
4. Reports with subreports are shown with a blue link. Click the link to drill down to the child reports.

Move the mouse over the bar charts and trend lines to show detailed values. The report that has focus shows the action menu: "Edit", "Clone", "Delete", and "Download".

## Default Reports

When you first access the Call Quality Dashboard portal, a default set of reports is automatically created. These reports are sometimes referred to as system reports. You are able to freely modify or delete these reports or extend them by creating new sibling and child reports.

At the top level, the "Audio Streams Monthly Trend" report shows the monthly trend for all audio streams. Move the mouse over the bars in a bar chart to show a more detailed view of the data represented by the bar chart. Click the title of the Audio Streams Monthly Trend report to navigate to the "Managed vs Unmanaged Audio Streams" report, where the reports are split between Managed and Unmanaged calls. Managed calls are calls made from inside the corporate firewall over wired connections. Unmanaged calls include calls made from outside the corporate firewall and all calls made over Wi-Fi.

The other top-level report is called the "User-reported Call Quality Rating Histogram." Call Quality Ratings are the numbers given by Skype for Business users at the end of a call to indicate the quality of the call. The rating numbers range from 1 to 5, 1 is the worst and 5 is the best. The histogram shows the number of audio calls that had the indicated rating in one month.

Click the title of any of the reports to navigate into reports with more filters on the data. In the system reports, each child report displays a subset of the data available in its parent report. The problem-solving model is simple: investigate which subreport the data or trend suggesting a problem is confined to, and gradually narrow down the problem space. The ability to create subreports allows you to investigate your own guesses about the cause of specific data trends.

## Create and Edit Reports

Click "Edit" in the action menu of a report to see the Report Editor. Each report is backed by a query into the cube. A report is a visualization of the data returned by its query. The Report Editor helps you edit these queries and the display options of the report. When you open the Report Editor, you see:



1. Dimensions, measures, and filters are chosen in the left pane. Hover over one of the existing values to show an "x" button that allows the value to be removed. Click the "plus" button next to a heading to open the dialog where you can add a new dimension, measure, or filter.
2. Options for chart customization are displayed at the top.
3. A preview of the report is available in the Report Editor.
4. A detailed report description can be created with the edit box at the bottom.

## Sparklines in Tables

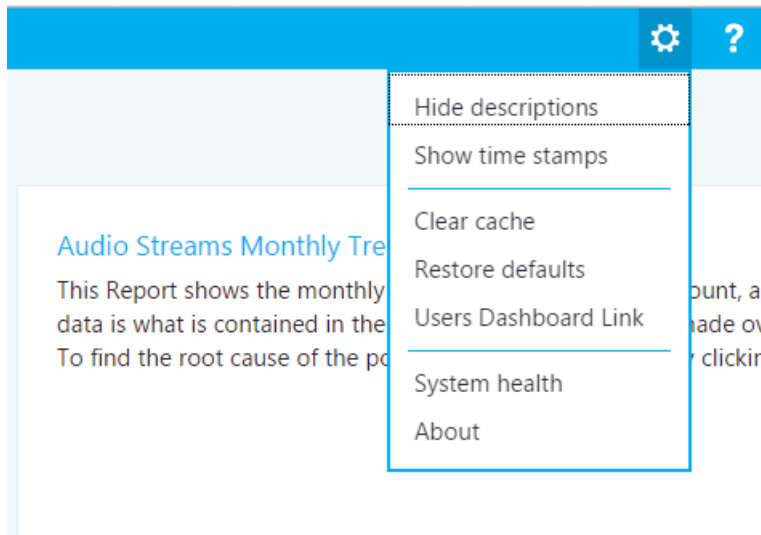
When StartDate.Month is added as a dimension and the data is rendered as a trend in table form, bar charts and sparklines can be shown inside the table cells. Move the mouse pointer over the bar chart and the sparklines to show the values for individual months.

User Agent Type	Month	Good	UnClassified	Poor	Poor%
Filter User Agent Type	Filter Month	Filter Go	Filter Un	Filter Po	Filter Po
	April 2015	458	2	36	7,287
	April 2015	54,088	68	294	0.541
	April 2015	3,042	4	12	0.393
	April 2015	52,316	205	166	0.316

In order for the bar charts and the sparklines to appear, the "Show sparklines" checkbox at the top of the Report Editor must be checked. This selects the Trend option and moves Month down to be the last dimension, which can also be accomplished by clicking on Month and using the up and down arrows to shift StartDate.Month up or down.

### Settings

The settings menu contains links to useful pages like the System Health and About pages, and is located in the top-right corner of the dashboard.



Whether to show descriptions and time stamps is up to individual users, and these settings only affect the individual's version of the dashboard, and do not modify the report set or what other users see. Clearing the cache causes all queries to reload their data from the cube, while restoring defaults deletes all of user-created or modified reports and recreates the system report set — what a user would see when they log in for the first time.

The Users Dashboard Link shows a page where users can view other users of CQD and browse their reports. To share a report set, copy the link in the URL bar and share it with another CQD user. This link is the same link other users would see in the Users Dashboard Link page under the user's username.

### Supplying Subnet Information

Additional information can be revealed if site-specific information is entered into the Archive database to provide subnet-to-building mapping information (for example, wired/wireless call quality by building).

At a minimum, complete the following tables to create these reports:

- CqdBuilding
- CqdNetwork

Additional information can be provided in CqdBuildingType and CqdBuildingOwnershipType tables to allow further filtering and drill-down.

The data used for these tables are defined as follows:

### CqdBuilding

COLUMN	DATA TYPE	ALLOW NULLS?	DETAILS
BuildingKey	int	No	Primary key for the CqdBuilding table.
BuildingName	varchar(80)	No	Building name.
BuildingShortName	varchar(10)	No	Shorter version of the Building name.
OwnershipTypeld	int	No	Foreign key, matches one of the entries in the CqdBuildingOwners table.
BuildingTypeld	int	No	Foreign key, matches one of the entries in the CqdBuildingType table.
Latitude	float	Yes	Latitude of the building.
Longitude	float	Yes	Longitude of the building.
CityName	varchar(30)	Yes	City name where the building is located.
ZipCode	varchar(25)	Yes	Zip code where the building is located.
CountryShortCode	varchar(2)	Yes	ISO 3166-1 alpha-2 codes for the country where the building is located.
StateProvinceCode	varchar(3)	Yes	Three-letter abbreviation for the State/Province where the building is located.
InsideCorp	bit	Yes	Bit indicates whether the building is part of the corporate network.
BuildingOfficeType	nvarchar(150)	Yes	Description of the building office type.
Region	varchar(25)	Yes	Region where the building is located.

### CqdNetwork

COLUMN	DATA TYPE	ALLOW NULLS?	DETAILS
Network	varchar(25)	No	Subnet address.

COLUMN	DATA TYPE	ALLOW NULLS?	DETAILS
NetworkRange	tinyint	Yes	Subnet mask.
NetworkNameID	int	Yes	Optionally maps to a row in CqdNetworkName table.
BuildingKey	int	Yes	Foreign key, matches one of the entries in the CqdBuilding table.
UpdatedDate	datetime	No	Datetime for when the entry was last updated.

By default this next table has one entry (0, 'Unknown').

### CqdBuildingType

COLUMN	DATA TYPE	ALLOW NULLS?	DETAILS
BuildingTypeId	int	No	Primary key for the CqdBuildingType table.
BuildingTypeDesc	char(18)	No	Building type description.

By default this next table has one entry (0, 'Unknown', 0, null).

### CqdBuildingOwnershipType

COLUMN	DATA TYPE	ALLOW NULLS?	DETAILS
OwnershipTypeId	int	No	Primary key for the CqdBuildingOwnershipType table.
OwnershipTypeDesc	varchar(25)	No	Ownership type description.
LeaseInd	tinyint	Yes	Index referencing another row in the CqdBuildingOwnershipType table, used for identifying leased buildings.
Owner	varchar(50)	Yes	Building owner.

By default this next table has one entry (0, 'Unknown', 0, null).

### CqdBssid

COLUMN	DATA TYPE	ALLOW NULLS?	DETAILS
bss	nvarchar(50)	No	Primary key for the CqdBssid table. Is the BSSID of the WiFi Access Point.
ess	nvarchar(50)	Yes	Wifi Access Point Controller information.
phy	nvarchar(50)	Yes	Phy information.
ap	nvarchar(50)	Yes	Wifi Access Point Name.
Building	nvarchar(500)	Yes	The Building Name the WiFi Access Point is located in.

## CQD Streams

A CQD stream is considered good, poor, or unclassified. CQM 1.5 now uses the following CQD definition:

- A poor stream is any combination of the poor call metrics beyond threshold.
- When one stream in a call is poor, both streams of the call are flagged poor. In conferences, each participant is counted as a unique call and is reported on independently of all others.
- Unclassified streams are streams without quality metrics (that is, Synthetic Transactions or short calls).
- Valid Streams = non-mobile clients
- Classifier cannot be modified

### Poor call definition/classifier

METRIC	THRESHOLD
DegradationAvg	Greater than 1.0 (-1 network MOS)
RoundTrip	Greater than 500
PacketLossRate	Greater than 0.1 (10%)
JitterInterArrival	Greater than 30
RatioConcealedSamplesAvg	Greater than 0.07

JPDR definition = Poor call definition minus RatioConcealedSamplesAvg

## Where is Caller/Callee?

CQD doesn't use Caller/Callee fields, instead it uses "First" and "Second" because there are intervening steps between the caller and callee.

**First** Will always be the Server endpoint (for example, AV MCU or Mediation Server) if a Server is involved in the stream.

**Second** Will always be the Client endpoint, unless it is a Server-Server stream.



## Example of First and Second classification

ENDPOINT 1 UATYPE	ENDPOINT 2 UATYPE	FIRST	SECOND
2 (AVMCU)	4 (Skype for Business)	Endpoint 1	Endpoint 2
2 (AVMCU)	1 (mMediationServer)	Endpoint 2	Endpoint 1
4 (Skype for Business)	4 (Skype for Business)	The Caller in MediaLine	The Callee in MMediaLine

If both endpoints are the same type, CQD makes the Caller entry First and the Callee Second. For more information about endpoint names, see [this blog](#).

## Accounting for VPN

If VPN solution is known to accurately set VPN flag, you're all set. Otherwise, use one of the following methods:

- Create a Network Type called VPN (preferred), then Associate VPN Subnets with this new VPN NetworkType.
- Create a building called VPN, then Associate VPN Subnets with this building.

## Query Fundamentals

A well-formed query contains all three of these parameters:

- Measurement
- Dimension
- Filter

An example of a well-formed query would be "Show me Poor Streams [Measurement] by Subnet [Dimension] for Building 6 [Filter]."

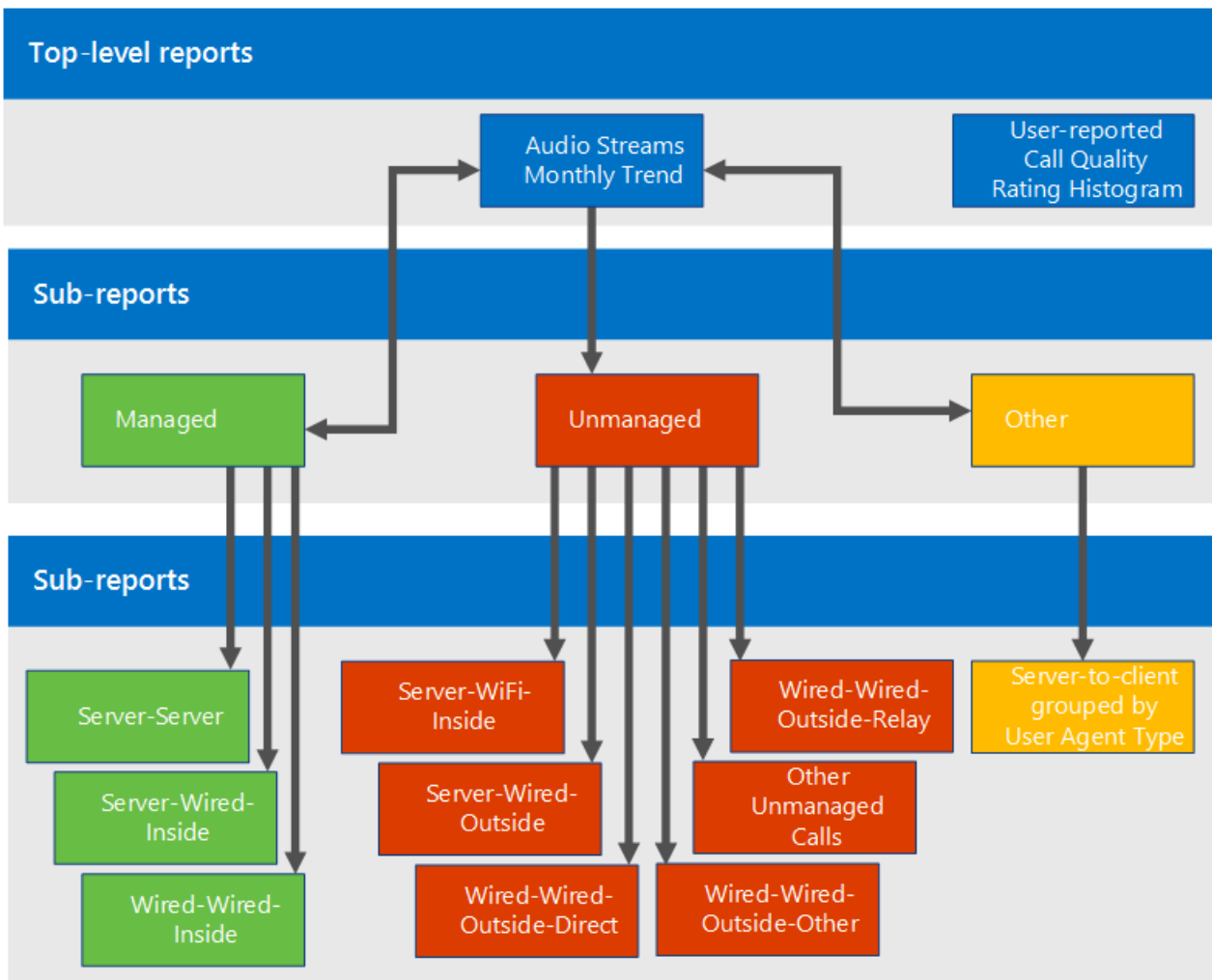
## What does UNION do?

Union allows you to filter conditions with the AND operator. There are scenarios where you can combine multiple Filter conditions together to achieve a result similar to an OR operation.

Example: To get all streams from a building, UNION provides a distinct view of the merged dataset. To use the UNION, insert common text into the UNION field on the two filter conditions you want to UNION.

## Default Report Breakdown

If Wireless is managed internally, you can recreate the Wireless reports in the Managed bucket.



## Operational Processes

Review and remediate Managed Streams first. Quality in this area should be 100% within your control and therefore easiest to remediate.

### Managed Streams

Review and remediate managed streams in the following order:

1. Server-Server
2. Server-Wired-Inside
3. Wired-Wired-Inside

### Unmanaged Streams

Review and remediate unmanaged streams in the following order:

1. Server-Wifi-Inside
2. Server-Wired-Outside
3. Server-Wifi-Outside
4. Wired-Outside-Direct
5. Wired-Outside-Relay
6. Other Unmanaged

# Statistics Manager for Skype for Business Server

5/20/2019 • 2 minutes to read

**Summary:** Read this topic to learn about Statistics Manager for Skype for Business Server, a powerful tool that allows you to view Skype for Business Server health and performance data in real time.

This section contains the following topics:

- [Plan for Statistics Manager for Skype for Business Server](#)
- [Deploy Statistics Manager for Skype for Business Server](#)
- [Upgrade Statistics Manager for Skype for Business Server](#)
- [Troubleshoot Statistics Manager for Skype for Business Server](#)

# Plan for Statistics Manager for Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Read this topic to learn about Statistics Manager for Skype for Business Server.

Statistics Manager for Skype for Business Server is a powerful tool that allows you to view Skype for Business Server health and performance data in real time. You can poll performance data across hundreds of servers every few seconds, and view the results instantly on the Statistics Manager Website.

You can use Statistics Manager to identify ongoing performance issues, view the results of a planned change to your environment, track resolution of outages, and much more. Out of the box, Statistics Manager is configured with Key Health Indicator (KHI) thresholds, and can be customized to suit your deployment's unique needs.

You can deploy Statistics Manager in an on-premises deployment in which a single server hosts all of the server-side Statistics Manager components. For more information about deploying Statistics Manager, see [Deploy Statistics Manager for Skype for Business Server](#). If you already have an existing deployment of Statistics Manager, but you have not yet upgraded to Release 2.0, see [What's new in Release 2.0](#) and [Upgrade Statistics Manager for Skype for Business Server](#).

This topic contains the following sections:

- [Features and capabilities](#)
- [What's new in Release 2.0](#)
- [Components](#)
- [On-premises deployment](#)
- [Requirements](#)
- [Security considerations](#)

## Features and capabilities

Statistics Manager allows you to:

- View raw data for all servers in real time. (Data is sampled at a very high rate and sent to the website in less than one second.)
- View data that is aggregated for a specific role; for example, Front End Server, Mediation Server, Edge Server, and so on.
- Drill down to view data for specific sites, specific pools within the site, and then specific servers within the pool.
- Create custom charts so that chosen counters are shown by default.
- Zoom and pan on both the x- and y- axes or on the x-axis only.
- Use date ranges or points in time to filter data.
- View server performance based on established key health indicators (KHIs). KHIs represent a collection of performance counters with a defined healthy range.

- View detailed metrics for each counter.
- Compare data across multiple populations or servers.
- View latent counter reports to identify agents that are not reporting current data to the dashboard service.
- Save a particular instance of chart data to a file.
- View KHIs in real time, including updates. If the history view is enabled, only new failures are shown.
  - View all KHIs at one time
  - View KHIs by server (Landscape view)
  - View KHI definitions

## What's new in Release 2.0

The following describes what's new in Release 2.0. If you have an existing deployment of Statistics Manager and you've not yet upgraded, see [Upgrade Statistics Manager for Skype for Business Server](#).

- Scenario views have been added for Edge Media, Fabric Health, Pool Failover and Registration scenarios.
- Many new counters have been added for SQL servers, more Skype for Business usage counters, and so on.
- Watcher node integration for the Statistics Manager Agent - if the Agent is installed on a watcher node, it will report synthetic transaction statistics as counters back to Statistics Manager.
- Numerous reliability and performance improvements.

To verify the version of the Statistics Manager Website you are running:

- In File Explorer, open (default directory) C:\Program Files\Skype for Business Server StatsMan WebSite\bin
- Right click on StatsManHubWebSite.dll and view its properties
- The product version will be shown in the Description details.

## Components

Statistics Manager consists of the following components:

- **Agent.** A lightweight agent that runs on each monitored server. The Agent allows configurable high rate polling of performance counters with local aggregation.
- **Listener.** The server side API that receives data from all Agents, and aggregates data across populations.
- **Hub.** Serves as the client API for the system, runs on the web server(s), and provides real-time data updates to clients connected via the website. (The Hub is automatically installed as part of the Website msi.)
- **Website.** A user interface that pulls together all the features available in the system.

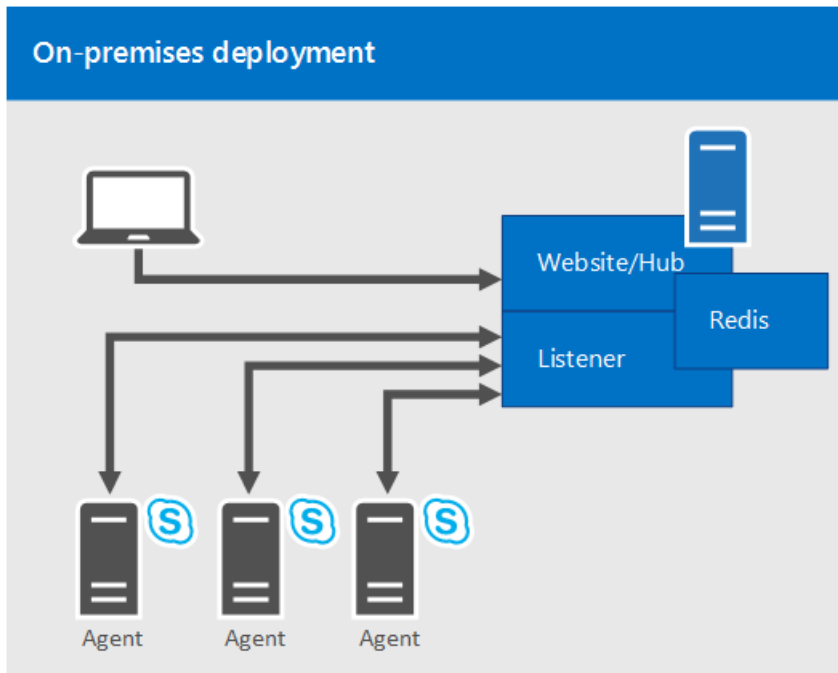
In addition, Statistics Manager requires **Redis**, an open-sourced data structure server for in-memory caching. For more information about downloading Redis, see [Deploy Statistics Manager](#).

## On-premises deployment

In an on-premises deployment, a single server hosts all of the server-side Statistics Manager components.

The following diagram shows an on-premises deployment, in which the Statistics Manager Website, Hub, Listener,

and Redis caching system are hosted on a single machine. Statistics Manager is monitoring three Skype for Business servers, each of which have a single Agent transmitting data to the Listener. Users connect to a single Website to view all data aggregated by Statistics Manager:



## Requirements

You will need to consider the following software, networking, and hardware requirements before you deploy Statistics Manager.

### Software requirements

- Windows Server 2016 and 2019
- IIS (automatically installed)
- Redis
- Statistics Manager services (automatically installed)
- PSEXec - Required to do remote agent deployment
- .NET 4.5 (included with 2012 R2) - Required for agents and server-side components
- Download the [Skype for Business Server, Real-Time Statistics Manager \(64-bit\)](#)

### Networking requirements

HOSTING SERVER	AGENTS	LISTENER
Minimum gigabit full duplex networking.	Outbound TCP port 8443 (customizable port number) to communicate with the Listener.	The Listener port must be the same on all servers.
Inbound TCP port 80 or 443 open to host the website.		
Inbound TCP port 8443 (customizable port number) for the agents to communicate with it.		

During installation, firewall ports for the Listener and the Website are automatically created. For the Agents, the installation assumes that outbound TCP connections are allowed by default.

### Hardware requirements

In an on-premises deployment, in which a single server hosts all of the server-side Statistics Manager components, a server with 16 GB of RAM and 4 CPU's should be able to support about 150 samples per second on average. To determine how many counters/agents you can support, use the following calculation:

$100 \text{ servers} * 80 \text{ counters} * 1 \text{ sample per minute from each agent} / 60 \text{ seconds} = \sim 133 \text{ samples per second.}$

## Security considerations

All traffic between servers is encrypted.

- Encrypted HTTPS traffic will be sent over port 8443 (by default) from the Agent to the Listener server.
- The Agent will verify the SSL thumbprint on the server to ensure the Listener server is the expected recipient. Note that the Agent uses certificate thumbprint verification (instead of chain verification). It will not do full certificate validation because it is possible to use self-signed certificates.
- After the Agent is satisfied the Listener is authentic, a password will be presented by the Agent which is then verified by the Listener.
- The Agent begins transmitting performance data over the connection to the Listener.

## For more information

For more information, see the following:

- [Deploy Statistics Manager for Skype for Business Server](#)
- [Upgrade Statistics Manager for Skype for Business Server](#)
- [Troubleshoot Statistics Manager for Skype for Business Server](#)

# Deploy Statistics Manager for Skype for Business Server

5/20/2019 • 9 minutes to read

**Summary:** Read this topic to learn how to deploy Statistics Manager for Skype for Business Server.

Statistics Manager for Skype for Business Server is a powerful tool that allows you to view Skype for Business Server health and performance data in real time. You can poll performance data across hundreds of servers every few seconds, and view the results instantly on the Statistics Manager Website.

Before you attempt to install Statistics Manager, be sure you are familiar with the software, networking, and hardware requirements. For more information, see [Plan for Statistics Manager for Skype for Business Server](#).

## NOTE

If you are upgrading from a previous version of Statistics Manager, see [Upgrade Statistics Manager for Skype for Business Server](#).

## NOTE

The Statistics Manager Website has been tested and works correctly on Internet Explorer 11+, Edge 20.10240+ , and Chrome 46+ (current evergreen version).

You can find the Statistics Manager downloadable at <https://aka.ms/StatsManDownload>.

This topic contains the following sections:

- [Deploy Statistics Manager](#)
- [Troubleshoot your deployment](#)
- [Create a self-signed certificate](#)

## Deploy Statistics Manager

To deploy Statistics Manager, follow these steps:

1. Prepare the Listener host machine by installing the Redis in-memory caching system, and by ensuring that you have installed the appropriate certificates.
2. Install the Listener service on the host machine.
3. Install the Website on the host machine.
4. Install an Agent on each Skype for Business Server machine you wish to monitor.
5. Import the topology for the servers you are monitoring.



## NOTE

Redis, the Listener service, and the Website must all be installed on the same host machine. Be sure the host machine does not have Skype for Business Server installed.

### Prepare the Listener host machine

To prepare the host machine, you will need to install the Redis in-memory caching system, and ensure that a valid certificate is on the machine. Microsoft recommends that you install the latest stable build of Redis 3.0. Statistics Manager version 2.0 was tested with Redis 3.2.100.

1. Download Redis from the following site: <https://github.com/Microsoft/redis>.

Unsigned installers can be downloaded from <https://github.com/Microsoft/redis/releases>

If required, signed binaries are available through popular package managers: [Nuget](#) and [Chocolatey](#).

- Run the provided msi and follow the prompts.
- Do not check the box to add a firewall rule.

2. The Listener service requires a certificate. Microsoft strongly recommends that you have a certificate signed by a trusted certificate authority.

If you want to use a self-signed certificate--for testing purposes in a lab, for example--see [Create a self-signed certificate](#).

Note that the Agent uses certificate thumbprint verification (instead of chain verification). It will not do full certificate validation because it is possible to use self-signed certificates.

### Install the Listener service

Install the Listener service on the host machine by running the StatsManPerfAgentListener.msi and specifying the following:

1. Review the License Agreement, and if you agree, select **I accept the terms in the license agreement**, and then click **Next**.
2. On the next page, specify the following information:

- **Service Password:** This is the password the remote Agents will use to authenticate to the Listener service.
- **Service Port:** This is the HTTPS port number that the Listener will use to communicate with the Agents. During installation, this port will be allowed through the local firewall, a URL ACL will be created, and an SSL cert will be bound to this port. The default is 8443.
- **Certificate Thumbprint:** This is the certificate thumbprint the Listener will use to encrypt the HTTPS protocol. Network Service must have read access to the private key.

Click the **Select...** button to choose the thumbprint.

You can find the Certificate thumbprint by using Certificate Manager or by using the following PowerShell command:

```
Get-ChildItem -path cert:\LocalMachine\My
```

- **Install Dir:** This is the directory on which the binaries will be installed. You may change it from the default by using the **Browse...** button.

- **AppData Dir:** This is the directory where the Logs folder and other data will be stored. You may change it from the default. It will not be deleted on uninstall.

3. Click **Install**.

To validate the installation, perform the following steps:

1. Open a browser and navigate to `https://localhost:<service-port>/healthcheck/`

By default, the service port is 8443 (unless you specified another port).

2. To ensure the Listener has installed properly, look for the following:

- If the healthcheck page shows up, the Listener installation was successful.
- If the KnownServerCount is 1 or higher, the connection to Redis is established.
- After waiting a few minutes, and after at least one Agent has been installed, check to see that the ValuesWritten counter is incrementing.

### Install the Website

Install the Website on the host machine by running the StatsManWebSite.msi (included with [Skype for Business Server, Real-Time Statistics Manager \(64-bit\)](#)) and specifying the following:

1. Review the License Agreement, and if you agree, select **I accept the terms in the license agreement**, and then click **Next**.

2. On the next page, specify the following information:

- **Service Port:** This is the port number the web site will listen on. You can change it later by using IIS manager binding. During installation, this port will be allowed through the local firewall.
- **Install Dir:** This is the directory where the binaries will be installed. You may change it from the default by using the **Browse...** button.
- **AppData Dir:** This is the directory where the Logs folder and other data will be stored. You may change it from the default. It will not be deleted on uninstall.

3. Click **Install**.

To view the Website, open a browser, and navigate to: `http://localhost,webport>/`.

To view health information only, open a browser, and navigate to: `http://localhost:<webport>/healthcheck/`.

By default, the web port number is 8080. You can change the port binding of the website by using IIS manager.

The web installer adds a local security group, called StatsManWebSiteUsers. You can add accounts to this security group to grant access to the Website.

### Install the Agents

Install an Agent on each Skype for Business Server that you wish to monitor by running the StatsManPerfAgent.msi and specifying the following:

1. Review the License Agreement, and if you agree, select **I accept the terms in the license agreement**, and then click **Next**.

2. On the next page, specify the following information:

- **Service Password:** This is the password the remote agent will use to authenticate to the Listener service.
- **Service URI:** This is the URI where the Listener resides. It should use the `https://name:port` format.

You can use a NETBIOS name or a FQDN. You can use the name that is also specified as the **Subject** or **Subject Alternative Names** of the certificate on the Listener service, but this is not a requirement.

- **Service Thumbprint:** This is the thumbprint of the SSL certificate the Listener is using. The Agent will use this thumbprint to authenticate to the Listener. (It will not do full certificate validation because it is possible to use self-signed certificates.)
- **Install Dir:** This is the directory on which the binaries will be installed. You may change it from the default by using the **Browse...** button.
- **AppData Dir:** This is the directory where the Logs folder and the encrypted password.txt file will be stored. You may thanks change it from the default. It will not be deleted on uninstall.

### 3. Click **Install**.

If you are installing an Agent on numerous machines, you will probably want to do this in unattended mode. For example:

```
msiexec /l install.log /i StatsManPerfAgent.msi SERVICE_THUMBPRINT=<thumbprint> SERVICE_PASSWORD=<password> SERVICE_URI=https://<hostname>:<servicePort>/[INSTALLDIR=<directory>][DIR_STATSMANAPPDATA=<directory>]
```

## Import the topology

After Statistics Manager is installed and running, you need to import the Skype for Business Server topology so that Statistics Manager knows the Site, Pool, and Role of each server. To import your Skype for Business Server topology, you will use the [Get-CsPool](#) cmdlet to retrieve information about each pool in use in your organization, then import this information into Statistics Manager.

To import the Skype for Business Server topology, follow these steps:

1. On a host that has the Skype for Business Server PowerShell cmdlets:
  - a. Run the following command:

```
Get-CsPool | Export-Clixml -Path mypoolinfo.xml
```

- b. Copy the "mypoolinfo.xml" file to the server that runs the Listener.

2. On the host that runs the Listener:

- a. Run PowerShell.
- b. Navigate to the directory on which the Listener is installed. The default is:

```
cd C:\Program Files\Skype for Business Server StatsMan Listener
```

3. To confirm which servers are being added and updated, run the following command:

```
.\Update-StatsManServerInfo.ps1 -CsPoolFile <path to mypoolinfo.xml>
```

The following command enables you to view all options:

```
Get-Help .\Update-StatsManServerInfo.ps1 -Detailed
```

To see your currently imported server information, run the following script:

```
.\Get-StatsManServerInfo.ps1
```

If you would like to monitor servers that are not in your Skype for Business Server topology--an Exchange Server, for example--you can do a single-server import on the host that runs the Listener. To do a single-server import, follow these steps:

1. Navigate to the directory on which the Listener is installed. The default is:

```
cd C:\Program Files\Skype for Business Server StatsMan Listener
```

2. Run the following command:

```
.\Update-StatsManServerInfo.ps1 -HostName <hostname> -SiteName <name of site> -PoolName <poolName> -  
Roles <role1>[,<role2>,<roleN>]
```

## Troubleshoot your deployment

If an Agent fails to start, check for the following:

- Is the agent registered in Statistics Manager?
  1. Make sure you followed the instructions for importing the topology. See [Import the topology](#).
  2. If the Agent is on a server that is not listed in the topology (for example, the nodes in a SQL AlwaysOn cluster), you will need to add the Agent manually by following the instructions in [Import the topology](#).

- Can the Agent contact the Listener?

1. Make sure the Listener service is running.

If it is not running, make sure Redis is running, and then try to restart the Listener.

2. Make sure the port is open to the Listener service, and that the Agent computer can communicate with the port.

- To ensure that Statistics Manager is collecting data, you can check the CSV file as follows.

The following command retrieves the counter storage names:

```
.\PerfAgentStorageManager.exe -redis=localhost -a=listcounterstoragenames -mode=verbose | findstr /i  
processor
```

The next command retrieves the values for the specified counters:

```
.\PerfAgentStorageManager.exe -redis=localhost -a=getcountervalues -counter="\\*\Processor  
Information\% Processor Time_Mean_Mean\_Total" -file:all-processor.csv
```

For information about all the events you might see in the application event log, see [Troubleshoot Statistics Manager for Skype for Business Server](#).

## Create a self-signed certificate

Microsoft strongly recommends that you use a certificate signed by a trusted certificate authority. However, if you want to use a self-signed certificate for testing purposes, do the following:

1. From a PowerShell console while logged on as Administrator, type the following:

```
New-SelfSignedCertificate -DnsName StatsManListener -CertStoreLocation Cert:\LocalMachine\My
```

2. Type `certlm.msc`. This will open the Certificate Manager for the local machine.
3. Navigate to **Personal**, and then open **Certificates**.
4. Right click on **StatsManListener->All Tasks->Manage Private Keys...**
5. Click **Add**.
6. In the **Enter the object names to select** box, type the following: Network Service
7. Click **OK**.
8. Under **Full Control**, un-check the **Allow** check box. (Only Read access is necessary.)
9. Click **OK**.

## For more information

For more information, see the following:

- [Plan for Statistics Manager for Skype for Business Server](#)
- [Upgrade Statistics Manager for Skype for Business Server](#)
- [Troubleshoot Statistics Manager for Skype for Business Server B](#)

# Upgrade Statistics Manager for Skype for Business Server

5/20/2019 • 3 minutes to read

**Summary:** Read this topic to learn how to upgrade Statistics Manager for Skype for Business Server.

This topic describes how to upgrade an existing installation of Statistics Manager for Skype for Business Server—a powerful tool that allows you to view Skype for Business Server health and performance data in real time. You can poll performance data across hundreds of servers every few seconds, and view the results instantly on the Statistics Manager Website.

For more information about Statistics Manager and the new features in Release 2.0, see [Plan for Statistics Manager for Skype for Business Server](#) and [Deploy Statistics Manager for Skype for Business Server](#).

There are two methods for upgrading:

- **Automated upgrade.** This method uses an automated script. It is the easiest method and should be applicable to all upgrade scenarios.
- **Manual upgrade.** This method is provided as a backup plan in the unusual case that the automated upgrade fails.

## Prerequisites

Before you upgrade, be sure you have the following information:

- Active Listener Certificate Thumbprint
- Listener Service Password (entered on install of the listener and every agent)
- SSL Certificate configuration for the website

## Automated upgrade

The script will gather your current certificate information and listener password, uninstall the old version of the product, and then install the new version of the product. The Redis instance installed on the server will not be touched, so any data stored in the cache will be retained through the upgrade process.

1. Place the MSI files for the new version of the agent, listener and website along with the Update-StatsMan.ps1 script into a single folder on the Listener computer.
2. Open an administrative PowerShell window. Upgrade the Listener component:

```
.\Update-StatsMan.ps1 -Service Listener
```

### NOTE

The Statistics Manager service password will be displayed in clear text on the command line as it is passed to the installer. Be sure to shield your monitor as needed.

1. On running the script, you should be prompted to uninstall the old version of the product. Answer Yes.

2. If the Listener service is running, you will be prompted to close the application before continuing. Allow the application to close (the Statistics Manager Listener service will be stopped).
3. Continue the install process. You should notice that the service password and certificate thumbprint are pre-populated. If not, add the values you saved before continuing.
4. Open an administrative PowerShell window. Upgrade the Website component:

```
.\Update-StatsMan.ps1 -Service Website
```

5. On running the script, you should be prompted to uninstall the old version of the product. Answer Yes.
6. If the Agent service is running, you will be prompted to close the application before continuing. Allow the application to close (the StatsMan Agent service will be stopped).
7. Continue the install process. You should notice that the service password and certificate thumbprint are pre-populated. If not, add the values you saved before continuing.
8. Open an administrative PowerShell window. Upgrade the Agent component:

```
.\Update-StatsMan.ps1 -Service Agent
```

9. On running the script, you should be prompted to uninstall the old version of the product. Answer Yes.
10. Continue the install process. You should notice that the website port is pre-populated. If not, add the value you saved before continuing.
11. Verify the website is working as expected using the browser.

#### NOTE

The Agent upgrade can be used with the `-NoPrompt` switch. This will allow the uninstall/install process to run silently, allowing tools such as PSEXec to run the upgrade remotely on a large number of servers.

### Manual upgrade

If for some reason, the automated upgrade fails, you can always perform a manual upgrade as follows:

1. On the Listener computer, uninstall the Listener, Website and the Agent (if it was installed on this server) via the Programs and Features control panel.

#### NOTE

Keep Redis installed so that the data in the cache will then be maintained through the upgrade process.

2. Install the new versions of the components, including the values you saved above when prompted for them. For more information about installing components, see [Deploy Statistics Manager](#)

## For more information

For more information, see the following:

- [Plan for Statistics Manager for Skype for Business Server](#)
- [Deploy Statistics Manager for Skype for Business Server](#)
- [Troubleshoot Statistics Manager for Skype for Business Server](#)





# Troubleshoot Statistics Manager for Skype for Business Server

5/20/2019 • 5 minutes to read

**Summary:** Read this topic to troubleshoot your deployment of Statistics Manager for Skype for Business Server.

This topic describes how to troubleshoot your Statistics Manager deployment by describing events you might see in the application event log, and appropriate actions you might take to rectify the event. This topic contains the following sections:

- [Agent events](#)
- [Listener events](#)
- [Website issues](#)

## Agent events

- **1000** — Unable to setup processor limiter (Job Object) — Unknown reason
- **1001** — Process limiting isn't allowed on the process (probably already inside a Job Object)

The Agent runs inside of a Windows Job Object to automatically limit its memory footprint. If the agent will not start and these event entries are present in the event log, the Job Object is not able to be instantiated on the server. To work around this, the upper memory limit can be removed by changing a value in the config file:

```
C:\Program Files\Skype for Business Server StatsMan Agent\PerfAgent.exe.config
```

Search for "MaxProcessMemoryMB" and change the value to "0" as shown:

```
<setting name="MaxProcessMemoryMB" serializeAs="String"> <value>300</value> </setting>
```

### NOTE

If this change is made, the Agent will generally still consume < 100 MB of memory, however it will not be forcefully limited to 300 MB as is the default. If this change is made, we recommend closely monitoring memory usage to ensure the Agent does not consume a large amount of memory on its host machine.

- **2000** — Client initialization failure
- **2001** — No connection could be made to the service on any source IP

If the Agent cannot connect to the Listener computer, check the following:

1. Ensure the Listener service is running on the Listener computer. If not, ensure Redis is running on that server and then restart the Listener service.

Check the Statistics Manager event log on the Listener computer to ensure there are no issues with the Statistics Manager Listener service itself.

2. Use a connectivity tool such as telnet to verify connectivity from the Agent computer to the Listener on the correct port.

If not, make sure the incoming firewall rule is enabled on the Listener computer for the network type that the Listener computer is connected to (private/public/domain). If the Listener computer is not joined to a domain, the network may be listed as public and in that case the firewall rules installed with Statistics Manager will not apply by default.

- **4000** — Failure to download Server Info from Listener (unknown reason)

- **4001** — Server Not Found in Listener Topology

This error will occur if the server is successfully connecting to the Listener, but the server was not added to the topology in the Listener's cache. Resolution options:

- Make sure you followed the instructions for importing the topology. See [Import the topology](#).
- If the Agent is on a server that is not listed in the topology (for example, the nodes in a SQL AlwaysOn cluster), you will need to add the Agent manually by following the instructions in [Import the topology](#).

- **4002** — Invalid Listener Password

The encrypted password that the agent is attempting to use does not match the service password on the Listener itself. Uninstall the Agent and re-install it using the correct service password.

- **4003** — Certificate Thumbprint Mismatch

The certificate thumbprint given to the Agent at install time does not match the thumbprint on the certificate the Listener is currently using and therefore the connection will be refused. Uninstall the Agent and re-install it using the correct certificate thumbprint.

- **4004** — Invalid Response or HttpStatusCode

The Listener is not responding with an expected status.

- If the connection is proxied, check the proxy configuration.
- Check the Listener computer's StatsMan log for issues with its configuration.

- **4005** — Couldn't de-serialize the XML

The server info on the Listener server is corrupt or there may be a version mismatch between the Agent and the Listener computers. Ensure the versions match and check the Listener event log for issues.

## Listener events

- **10000** — Startup failure Unknown reason (these are unrecoverable and the service will stop/crash as a result)

- **10001** — Configuration problem

Generally this will occur when the [listener\_install\_location]\PerfAgentListener.exe.config file has been modified by hand and cannot be read by the application.

- **10002** — HTTP Listener initialization error

This event will generally be logged when the URL ACL has not been set properly during installation or the SSL Cert is invalid. Ensure the certificate in your configuration is valid. If it is, reinstall the Listener according to the instructions in [Deploy Statistics Manager](#).

- **10003** — Redis failure
- **10004** — Caching infrastructure failure
- **10007** — Settings (stored in redis)

The Listener could not contact Redis or retrieve well-formed data from the cache and could not start. Ensure the Redis service is started and configured properly on the server.

- **10005** — Server info retrieval/parsing

The topology information in the Redis cache is invalid. First, attempt to restart Redis and the Listener. If the error persists, see [Import the topology](#) to recreate the topology data.

- **10100** — Redis PING outage
  - **10101** — Redis PING continued outage (every 60 seconds)
  - **30100** — Redis PING outage restored

These will be logged when the Listener cannot connect to Redis. Ensure Redis is started and network connectivity between the Listener and Redis is available.

- **10200** — Redis Write outage
  - **10201** — Redis Write outage continued (every 60 seconds)
  - **30100** — Redis Write outage resolved

These will be logged when the Listener cannot write to the Redis cache. Ensure Redis is started and network connectivity between the Listener and Redis is available.

- **30000** — Successfully started

Logged each time the Listener is started.

- **22000** — Initialization of Statistics Manager Agent succeeded.
- **23000** — Initialization of EventLogQueryManager succeeded (first time or after failing)
- **24000** — Initialization of serverinfo succeeded (first time or after failing)
- **25000** — Listener is back online after failing to post (or first successful post)
- **5000** — Start of listener offline for posting data
- **5001** — Listener is still offline for an extended period

These events can be useful for monitoring/alerting/clearing issues.

## Website issues

- Repetitive login prompts in Chrome - this was a bug that has been resolved in version 1.1. Be sure you have upgraded to the latest version of Statistics Manager if you are seeing repeated login prompts in the Chrome browser. To verify the version of the website you are running:
  - In File Explorer, open (default directory)
  - Right click on StatsManHubWebSite.dll and view its properties.
  - If a computer cannot be found in the KHI Landscape view or the Counter Details view, make sure it is a member of a Site and a Pool. If it is not, it will not appear in those views. For information about defining a site and pool for a server in the topology, see [Import the topology](#).

- The product version will be shown in the Description details.

## For more information

For more information, see the following:

- [Plan for Statistics Manager for Skype for Business Server](#)
- [Deploy Statistics Manager for Skype for Business Server](#)
- [Upgrade Statistics Manager for Skype for Business Server](#)

# Manage Skype for Business Server 2019 using SCOM Management pack

9/30/2019 • 13 minutes to read

**Summary:** Learn how to configure your Skype for Business Server 2019 infrastructure to work with System Center Operations Manager.

In an ideal world, you'd never encounter issues with Skype for Business Server 2019. However, Skype for Business Server can be affected by external factors—for example, network crashes and hardware failures. By using Skype for Business Server 2019 Management Packs, you can identify and address potential issues proactively. In this way, the Skype for Business Server 2019 Management Packs extend the capabilities of System Center Operations Manager.

This information was written based on version 9319.0 of the Monitoring Pack for Skype for Business Server 2019 communications software.

## Configuration overview

To configure your Skype for Business Server 2019 infrastructure to work with System Center Operations Manager, you must do three things:

Identify and [Configure the Primary Management Server](#). To do this, you must install System Center Operations Manager 2012 SP1 or R2.

Identify and [Configure the Skype for Business Server computers that will be monitored](#). To monitor a Skype for Business Server computer by using System Center Operations Manager, you must install the System Center Operations Manager agent files, and configure each server to act as a proxy.

Identify and [Install and configure watcher nodes](#). Watcher nodes are computers that periodically run Skype for Business Server synthetic transactions—Windows PowerShell cmdlets that verify that key Skype for Business Server components, such as the ability to log on to the system or the ability to exchange instant messages, are working as expected.

## System Center Operations Manager Root Management Server and Agent Support

The Management Packs can be used with System Center Operations Manager 2007 R2 (64-bit) (Supported for Migration purposes only) or System Center Operations Manager 2012 SP1 & R2 (64-bit). The following table shows the supported configurations for the Management Packs for Skype for Business Server 2019:

CONFIGURATION	SUPPORTED?
Windows Server 2008 R2 operating system Windows Server 2012 R2 operating system	Yes. Both on Skype for Business Server 2019 server and synthetic transaction watcher nodes.
Clustered servers	Not supported.
Agentless monitoring	Not supported.
Virtual environment	Yes.

CONFIGURATION	SUPPORTED?
Domain-joined server roles	All internal Skype for Business Server 2019 server roles must be domain-joined.
Stand-alone server roles	Skype for Business Server 2019 Edge Servers are not required to be domain-joined.
Topology limitations	All server roles in a deployment must be monitored from the same Operations Manager Management Group.
Synthetic transactions watcher node	Monitoring scenario availability with a synthetic transactions watcher node is supported (additional configuration required). Watcher nodes are not required to be domain-joined.

The following table shows the capacity and operating system requirements for a synthetic transaction watcher node:

HARDWARE COMPONENT	MINIMUM REQUIREMENT
CPU	One of the following: 64-bit processor, quad-core, 2.33 GHz or higher 64-bit 2-way processor, dual-core, 2.33 GHz or higher
Memory	8 GB
Operating system	Windows Server 2008 R2 Windows Server 2012 R2
Network	1 network adapter at 1 Gbps

## Prerequisites

To run a synthetic transaction watcher node, you must first install the following:

- System Center Operations Manager Agent
- Microsoft .NET Framework 4.5
- Skype for Business Server core installation files (OcsCore.msi) and Unified Communications Managed API (UCMA) (versions must match the Skype for Business Server WatcherNode.msi version)

## Files in this Monitoring Pack

The Monitoring Pack for Skype for Business Server 2019 includes the following files:

- Microsoft.LS.2019.Monitoring.ActiveMonitoring.mp
- Microsoft.LS.2019.Monitoring.ComponentAndUser.mp
- WatcherNode.msi

## What's New

The following features are new to Skype for Business Server 2019 Management Packs.

- **Changes in Sept 2019 update** Some alerts have had special characters removed. In some cases special

characters interfere with the SCOM command channel notification feature.

- **Automatic discovery for Client Sign-In** Client applications that sign-in to Skype for Business Server 2019 often automatically discover the server to sign-in to. Synthetic transactions now support verification that automatic discovery is configured correctly.
- **Customized synthetic transaction run intervals** To simplify the set up process of Watcher Nodes, synthetic transactions can share user accounts. This slows down the frequency at which the tests are run as the tests are serialized to avoid conflicts. By default, synthetic transactions run every 15 minutes to ensure all tests have time to run. Administrators who choose to use more users or fewer tests per user may now reduce the run interval, as well.
- **Video Interop Services synthetic transaction** Customers who are migrating to Skype for Business Server 2019 from other vendor solutions often desire to continue using the video teleconferencing devices (VTCs) from these other vendors. Video Interop Server is a new Skype for Business Server 2019 server role that enables customers to continue to use Cisco VTCs in their conference rooms by connecting to Cisco CUCM via a video SIP trunk. This feature also adds a synthetic transaction to help verify that the Video Interop Server is up and can handle incoming connections over a video SIP trunk.
- **Application Sharing Conferencing synthetic transaction** End-to-end scenario validation for Application Sharing Conferences is now supported.

## Monitoring Scenarios

The Skype for Business Server 2019 Management Pack leverages a variety of features to help you detect and diagnose issues. These features provide real-time visibility into the health of a Skype for Business Server 2019 environment.

MONITORING SCENARIO	DESCRIPTION
Synthetic transactions	Windows PowerShell cmdlets to test and help ensure high availability of scenarios such as sign in, presence, IM, and conferencing for users. The synthetic transactions can be run from any geographic location including inside the enterprise, outside of the enterprise and in branch offices. When a synthetic transaction fails, HTML logs are created to help determine the exact nature of the failure. This includes understanding which action failed, the latency of each action, the command line used to run the test, and the specific error that occurred.
Call reliability alerts	Call Detail Records (CDRs) written by Skype for Business Server 2019 Servers reflect whether users are able to connect to a call or why a call is terminated. Call reliability alerts query the CDR database to produce alerts that indicate when a high number of users experience connectivity issues for peer-to-peer calls or basic conferencing functionality. Scenario coverage includes audio calls, peer-to-peer instant messaging (IM) and other conferencing features.
Media quality alerts	Database queries that look at Quality of Experience (QoE) reports published by Skype for Business Server 2019 clients at the end of each call. These queries produce alerts that pinpoint scenarios where users are most likely to experience compromised media quality during calls and conferences. The data is built on key metrics, such as packet latency and loss, which directly contribute to the quality of user experience.

MONITORING SCENARIO	DESCRIPTION
Component health alerts	Individual server components raise alerts via event logs and performance counters to indicate failure conditions that may significantly affect user scenarios. These alerts indicate a variety of conditions, such as services not running, high failure rates, high message latency, or connectivity issues.
Dependency health monitoring	Skype for Business Server can fail for a variety of external reasons. The Management Pack monitors and collects data for critical external dependencies that can indicate severe issues. These dependencies include Internet Information Services (IIS) availability, and CPU of servers used for Skype for Business Server.

### Alert Prioritization

Alerts are classified into the following categories:

**High Priority alerts:** These alerts indicate conditions that cause service outages for large groups of users and require immediate action. Outages detected by synthetic transactions and offline services (such as Skype for Business Server Audio/Video Conferencing) qualify as High Priority alerts. In contrast, a component failure on a single machine is not a High Priority alert. Skype for Business Server 2019 has built-in high-availability features for these situations—for example, multiple Front End Servers behind load balancers.

**Medium Priority alerts:** These alerts indicate conditions that affect a subset of users or indicate issues in call quality—for example, component failures, latency in call establishment, or lower audio quality in calls. Alerts in this category are stateful (that is, the nature of the alert changes based on the state of the network connection.) For example, if call establishment times indicate latency but then return to a normal threshold, this Medium Priority alert would be auto-resolved in System Center Operations Manager and administrators would not need to take action. Alerts that cannot be auto-resolved are typically addressed by administrators on the same business day.

**Other alerts:** These alerts are generated from components that might affect a specific user or subset of users. For example, a typical alert would be that the Address Book service could not parse the Active Directory® Domain Services (AD DS) entry for user: testuser@contoso.com. Administrators can address these alerts whenever they have time available.

### Synthetic Transactions

Skype for Business Server 2019 Management Packs provide increased coverage for alerts through synthetic transactions. Synthetic transactions are Windows PowerShell cmdlets integrated into the Operations Manager management pack to test end-to-end user scenarios. When you designate a server to execute synthetic transactions, these cmdlets are triggered periodically by the management pack. Failures resulting from a synthetic transaction generate a stateful alert. Here are supported synthetic transactions for Skype for Business Server 2019:

#### Supported Synthetic Transactions for Registration, Presence, and Contacts

1	Registration (user login)	Available Lync Server 2010 and beyond
2	Address Book Service (file download)	Available Lync Server 2010 and beyond
3	Address Book Web Query	Available Lync Server 2010 and beyond
4	Presence	Available Lync Server 2010 and beyond
5	Unified Contact Store	Available Lync Server 2013 and beyond



## Supported Synthetic Transactions for Peer-to-Peer Services

6	Peer-to-Peer Instant Messaging	Available in Lync Server 2010 and beyond
7	Peer-to-Peer Audio Video	Available in Lync Server 2010 and beyond
8	MCX Peer-to-Peer Instant Message (mobile)	Available in the September 2011 release of Lync Server 2010 to Skype for Business 2019

### NOTE

MCX (Mobility Service) support for legacy mobile clients is no longer available in Skype for Business Server 2019. All current Skype for Business mobile clients already use Unified Communications Web API (UCWA) to support instant messaging (IM), presence, and contacts. Users with legacy clients using MCX will need to upgrade to a current client.

## Supported Synthetic Transactions for Conferencing and Persistent Chat

9	Audio Video Conferencing	Available in Lync Server 2010 and beyond
10	Data Conferencing	Available in Lync Server 2013 and beyond
11	Instant Message Conferencing	Available in Lync Server 2010 and beyond
12	Persistent Chat	Available in Lync Server 2013 and beyond
13	Join Launcher (scheduled meetings)	Available in Lync Server 2013 and beyond
14	Dial in Conferencing	Available in Skype for Business Server 2015 and beyond
15	Application Sharing Conferencing	Available in Skype for Business Server 2015 and beyond
16	UCWA Conference (web meeting join)	Available in Skype for Business Server 2015 and beyond

## Supported Synthetic Transactions for Network and Partner Dependencies

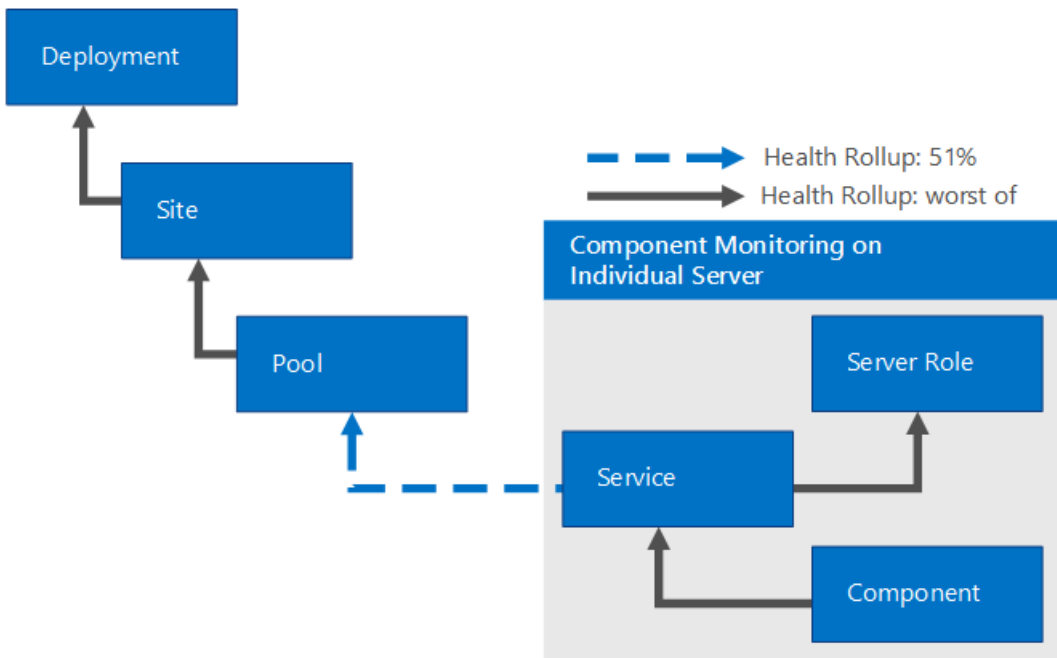
17	AV Edge Connectivity	Available in Lync Server 2013 and beyond
18	AV Edge Connectivity Exchange Unified Message Connectivity (voicemail)	Available in Lync Server 2013 and beyond

19	PSTN Peer-to-Peer Call	Available in Lync Server 2010 and beyond
20	XMPP Instant Messaging (federation)	Available in Lync Server 2013 and beyond
21	Video Interop Server	Available in Skype for Business Server 2015 and beyond

## How Health Rolls Up

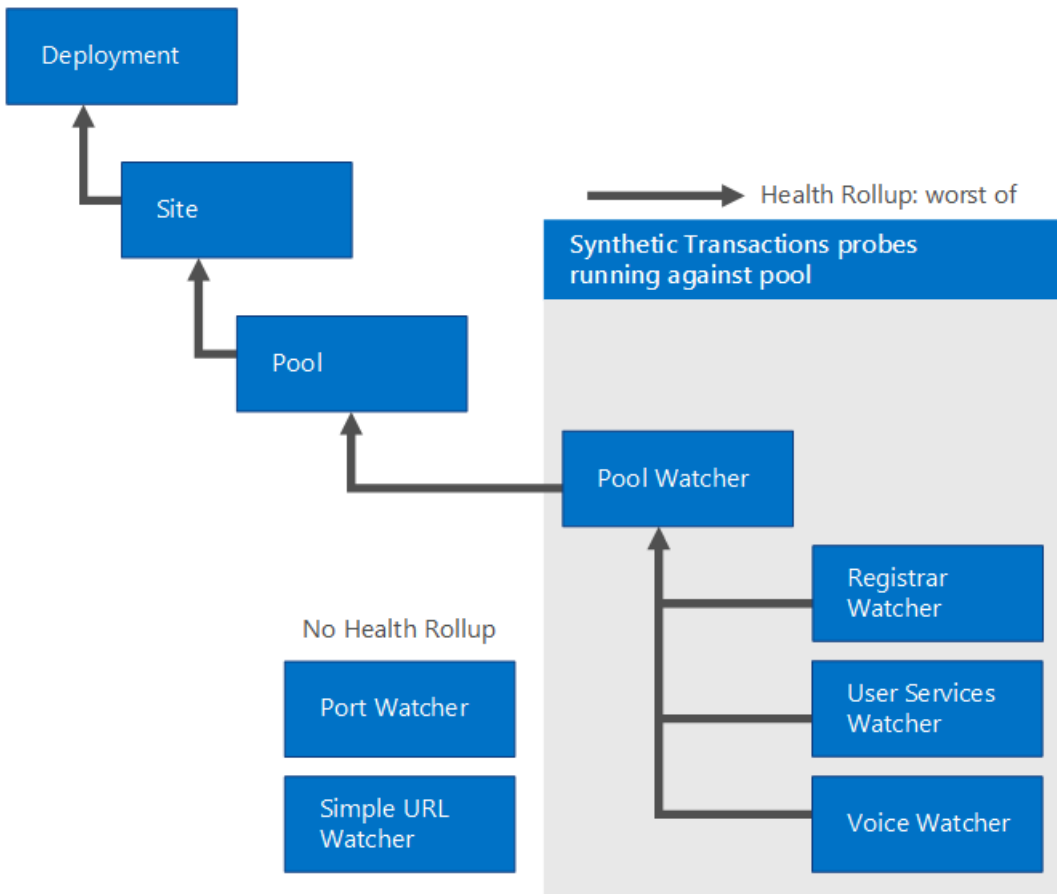
The following Table shows the health states of objects the Skype for Business Server monitoring pack.

MANAGEMENT PACK OBJECT	DESCRIPTION
Skype for Business Server Deployment	Represents the deployment of Skype for Business Server 2019 in the organization.
Skype for Business Server Site	Represents different geographical locations where services are deployed.
Skype for Business Server Pool	A Pool (within a Site) that provides communications services, such as instant messaging and conferencing, to users. Applicable to Front End pools, Edge pools, and Director pools, even if there is only a single machine in a given pool.
Skype for Business Server Role	A server role that hosts Skype for Business Server Service.
Skype for Business Server Service	Represents a functionality deployed on a specific machine (for example, user service on fp01.contoso.com).
Skype for Business Server Component	A component of the Service (for example, the Address Book Download component is a part of the Web Service).
Skype for Business Server Pool Watcher	An instance of synthetic transactions that are running against one pool.
Skype for Business Server Registrar Watcher	An instance of synthetic transactions that run against one Registrar pool.
Skype for Business Server User Services Pool Watcher	An instance of synthetic transactions that run against one User Services pool.
Skype for Business Server Voice Pool Watcher	An instance of synthetic transactions that run against one Voice pool.
Skype for Business Server Port Watcher	An instance of Port checks running against one pool.
Simple URL Watcher	Performs HTTPS probing of the configured simple URLs in a deployment.



A Skype for Business Server pool can contain multiple individual Skype for Business Server systems (with more than one Skype for Business Server role, Skype for Business Server service, and Skype for Business Server component). Therefore, the failure of an individual server or component is less critical to the overall health of the Skype for Business Server pool, because other servers in the same pool can provide the application service to the client. The health will roll up on a percentage level to the Skype for Business Server pool.

The Skype for Business Server Pool Watcher performs synthetic transactions against a Skype for Business Server pool. Consecutive failure of one or more synthetic transactions (a process known as the consecutive polling interval) will roll up the critical health state to the pool level (worst of any synthetic transaction), as shown in the following diagram.



Best Practice: Create a Management Pack for Customizations

By default, Operations Manager saves all customizations, such as overrides to the Default Management Pack. As a best practice, you should create a separate management pack for each sealed management pack that you want to customize.

When you create a management pack for storing customized settings for a sealed management pack, we recommend naming the new management pack appropriately, such as "Skype for Business Server 2019 Customizations."

Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. This also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

## Links

The following links connect you to information about common tasks that are associated with System Center 2012 Monitoring Packs:

- [Management Pack Life Cycle](#)
- [How to Import a Management Pack in Operations Manager 2012](#)
- [How to Override a Rule or Monitor](#)
- [How to Create a Run As Account in Operations Manager 2012](#)
- [Managing Run As Accounts and Profiles](#)
- [How to Export an Operations Manager Management Pack](#)
- [How to Remove an Operations Manager Management Pack](#)

The following links connect you to information about common tasks that are associated with System Center 2007 Monitoring Packs:

- [Administering the Management Pack Life Cycle](#)
- [How to Import a Management Pack in Operations Manager 2007](#)
- [How to Monitor Using Overrides](#)
- [How to Create a Run As Account in Operations Manager 2007](#)
- [How to Modify an Existing Run As Profile](#)
- [How to Export Management Pack Customizations](#)
- [How to Remove a Management Pack](#)

For questions about Operations Manager and monitoring packs, see the [System Center Operations Manager community forum](#).

A useful resource is the [System Center Operations Manager Unleashed](#) blog, which contains "By Example" posts for specific monitoring packs.

For additional information about Operations Manager, see the following blogs:

- [Operations Manager Team Blog](#)
- [Kevin Holman's OpsMgr Blog](#)

- [Thoughts on OpsMgr](#)
- [Raphael Burri's blog](#)
- [BWren's Management Space](#)
- [Ops Mgr ++](#)

**IMPORTANT**

All information and content on non-Microsoft sites is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.

## See also

[Skype for Business Server 2019 Management Tools](#)

# Configure the Primary Management Server

5/20/2019 • 4 minutes to read

**Summary:** Configure your primary management server, install System Center Operations Manager, and import management packs for Skype for Business Server 2019.

To take full advantage of the new health monitoring capabilities included in Skype for Business Server 2019, you must first designate a computer to act as your primary management server. You must then install System Center Operations Manager 2012 SP1 or R2 or System Center Operations Manager 2007 R2 on that computer. In addition, you must first install a supported version of SQL Server to function as your Operations Manager back-end database.

When you install System Center Operations Manager, you will need to install all the components of that product, including:

- Operational database
- Server
- Console
- Windows PowerShell cmdlets
- Web console
- Reporting
- Data warehouse

## IMPORTANT

The "[Microsoft Report Viewer 2010 Redistributable Package](#)" needs to be installed before you install System Center Operations Manager 2012.

For details about these products and their installation, see the following links:

- [System Center Operations Manager 2012](#)
- [System Center Operations Manager 2007](#)

Keep in mind that you can have only one Root Management Server per Skype for Business Server deployment.

## Importing the Skype for Business Server 2019 Management Packs

You can extend the capabilities of System Center Operations Manager by installing management packs—software that dictates which items System Center Operations Manager can monitor, how those items should be monitored, and how alerts should be triggered and reported. Skype for Business Server 2019 includes two System Center Operations Manager management packs that provide the following capabilities:

- **The Component and User Management Pack** (Microsoft.LS.2019.Monitoring.ComponentAndUser.mp) tracks Skype for Business Server issues recorded in event logs, registered by performance counters, or logged in the call detail records (CDRs) or the Quality of Experience (QoE) databases. For critical issues, System Center Operations Manager can be configured to immediately notify administrators through email, instant message, or SMS messaging. (SMS, or Short Message Service, is the technology used to send text

messages from one mobile device to another.)

#### NOTE

For details about configuring Operations Manager notification, see [Configuring Notification](#).

- **The Active Monitoring Management Pack** (Microsoft.LS.2019.Monitoring.ActiveMonitoring.mp) proactively tests key Skype for Business Server components, such as signing into to the system, exchanging instant messages, or making calls to a phone located on the public switched telephone network (PSTN). These tests are conducted by using the Skype for Business Server synthetic transaction cmdlets. For example, the **Test-CsIM** cmdlet is used to simulate an instant messaging conversation between a pair of test users. If this simulated conversation fails, an alert is generated.

Importing the management packs is a crucial step. If the management packs are not imported, you will not be able to use Operations Manager to monitor Skype for Business Server events or run Skype for Business Server synthetic transactions.

The Component and User Management Pack is used to monitor only Skype for Business Server 2019. If you are in a coexistence scenario where both Skype for Business Server 2019 and Skype for Business Server 2015 are installed, you should continue to use the Skype for Business Server 2015 management packs for your Skype for Business Server 2015 computers.

#### NOTE

Management packs for Skype for Business Server 2019 include the Skype for Business Server 2019 Component and User Management Pack and the Skype for Business Server 2019 Active Monitoring Management Pack.

You can use one of the following tools to import management packs:

- **System Center Operations Manager** With this method, you use the Operations Manager to add monitoring for Skype for Business Server.
- **Operations Manager Shell** You can use the Operations Manager Shell to import directly, or to troubleshoot any issues that you encounter when you import management packs by using the System Center Operations Manager console.

### Importing the Management Packs by Using System Center Operations Manager

1. Download the SkypeForBusiness2019ManagementPacks.msi from the Microsoft Web downloads, and install the msi.
2. In System Center Operations Manager, click **Administration**.
3. In the Administration pane, right-click **Management Packs**, and then click **Import Management Packs**.
4. In the **Select Management Packs** dialog box, click **Add**, and then click **Add from disk**.
5. In the **Online Catalog Connection** dialog box, click **No**.
6. In the **Select Management Packs to import** dialog box, locate and select the files Microsoft.LS.2019.Monitoring.ActiveMonitoring.mp and Microsoft.LS.2019.Monitoring.ComponentAndUser.mp, and then click **Open**. To select multiple files in the dialog box, click the first file, and then hold down the Ctrl key and click the subsequent files.
7. In the **Select Management Packs** dialog box, click **Install**. If you get an error message and installation fails, that typically means that the management pack files are in a folder protected by the Windows User Account Control. If this occurs, copy the files to a different folder, and then restart the import and installation

process.

8. In the **Select Management Packs** dialog box, click **Close**. The import and installation process might require several minutes to complete.

## Importing the Management Packs by Using the Operations Manager Shell

In general, it is easier to import the management packs by using the Operations Manager console. However, if an error occurs and the import fails, the console does not always provide adequate error reports. By comparison, the Operations Manager Shell provides detailed information. If you are using Operations Manager and you encounter issues when importing a management pack, import the pack by using the Operations Manager Shell. The information provided by Operations Manager Shell can help you determine why the import failed.

1. Click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Shell**.
2. In Operations Manager Shell, type the following command at the command prompt, using the actual path to your copy of the file Microsoft.LS.2019.Monitoring.ActiveMonitoring.mp, and then press ENTER:

```
Import-SCOMManagementPack -FullName "D:\MP\Microsoft.LS.2019.Monitoring.ActiveMonitoring.mp"
```

3. After you have imported the first management pack, repeat the process, using the path to your copy of the file Microsoft.LS.2019.Monitoring.ComponentAndUser.mp:

```
Import-SCOMManagementPack -FullName "D:\MP\Microsoft.LS.2019.Monitoring.ComponentAndUser.mp"
```



# Configure the Skype for Business Server computers that will be monitored

5/20/2019 • 3 minutes to read

**Summary:** Install the Operations Manager agent files on the Skype for Business Server 2019 computer to be monitored, and configure the computer to act as a System Center proxy.

Each Skype for Business Server 2019 computer that you want to monitor must be able to self-report its existence to the management server. To enable this process, you must install the Operations Manager agent files on each of the computers to be monitored. After installing the agent files, you must configure the computer to act as a System Center proxy. Be sure that you have first installed and configured Skype for Business Server on these computers before carrying out these procedures.

## Installing a Certificate on a Watcher Node Located Outside the Perimeter Network

System Center Operations Manager agents running in a perimeter network (such as a Skype for Business Server Edge Server), outside of the enterprise (such as an external synthetic transaction watcher node), or across an Active Directory trust boundary, may require the configuration of a System Center Operations Manager Gateway Server. This server role enables agents that do not have a trust relationship with the Root Management Server to raise alerts. For details, see [Managing Gateway Servers in Operations Manager 2012](#).

If you deploy an agent in one of these locations, you will also need to request and configure a certificate that enables the watcher node to send alerts to System Center Operations Manager. To simplify this process, the Operations Manager team has created a set of utilities that enable you to request and install the correct type of certificate on the watcher node computer. For details, and to download these utilities, see [Obtaining Certificates for Non-Domain Joined Agents Made Easy with Certificate Generation Wizard](#).

### Installing the Operation Manager Agent Files

1. On your System Center setup media, double-click **Setup.exe**.
2. In the System Center Operation Manager setup wizard, click **Install Operations Manager Agent**, from Install Agent under Optional Installations
3. In the System Center setup wizard, on the Welcome to the System Center Operations Manager Setup wizard page, click **Next**.
4. On the Destination Folder page, select the folder where the Operations Manager Agent files will be installed and click **Next**.
5. On the Management Group Configuration page, select **Specify Management Group information** and click **Next**.
6. On the Management Group Configuration page, type the name of your Operations Manager Management Group in the **Management Group Name** box, and then type the host name of your Operations Manager server (for example, atl-scom-001) in the **Management Server** box. If you changed the port number used by Operations Manager, enter the new port number in the **Management Server Port** box. Otherwise, leave the port at the default value of 5723, and then click **Next**.
7. On the Agent Action Account page, select **Local System** and click **Next**.
8. On the Microsoft Update page, select **I don't want to use Microsoft Update** and click **Next**.

9. On the Ready to Install page, click **Install**.
10. On the Completing the System Center Operations Manager Setup wizard page, click **Finish**.
11. Click **Exit**.

For System Center 2012, you can verify that the agent has been created by clicking **Start**, clicking **All Programs**, clicking **System Center Operations Manager 2012**, and then clicking **Operations 2012 Manager Shell**. In the Operations Manager Shell, type the following Windows PowerShell command, and then press ENTER:

```
Get-SCOMAgent
```

A list of all your Operations Manager agents will appear.

## Configuring the Skype for Business Server Computer to Participate in System Center Discovery

To make sure that your new Skype for Business Server agent participates in the discovery process for System Center Operations Manager, you must complete the following procedure on each computer where the System Center Operations Manager console has been installed:

1. On the Administration tab, click **Agent Managed**.
2. Click on **Discovery Wizard** and complete the wizard for the computer to be discovered.
3. Reboot the Health Agent service. Rebooting the service will force discovery of the new machine. If you do not reboot the service, it could take as long as 4 hours before the new machine is discovered by System Center Operations Manager.
4. Verify that no error events were recorded in the Operations Manager event log.
5. The computer where the agent is pushed successfully will be shown under "Agent Managed" list and the computer where agent was installed manually will be shown under "Pending Management", click on the computer name and approve.
6. Right-click the name of the computer, and then click **Properties**. In the Properties dialog box, on the Security tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**, and then click **OK**.

# Configure the Skype for Business Server computers that will be monitored

5/20/2019 • 3 minutes to read

**Summary:** Install the Operations Manager agent files on the Skype for Business Server 2019 computer to be monitored, and configure the computer to act as a System Center proxy.

Each Skype for Business Server 2019 computer that you want to monitor must be able to self-report its existence to the management server. To enable this process, you must install the Operations Manager agent files on each of the computers to be monitored. After installing the agent files, you must configure the computer to act as a System Center proxy. Be sure that you have first installed and configured Skype for Business Server on these computers before carrying out these procedures.

## Installing a Certificate on a Watcher Node Located Outside the Perimeter Network

System Center Operations Manager agents running in a perimeter network (such as a Skype for Business Server Edge Server), outside of the enterprise (such as an external synthetic transaction watcher node), or across an Active Directory trust boundary, may require the configuration of a System Center Operations Manager Gateway Server. This server role enables agents that do not have a trust relationship with the Root Management Server to raise alerts. For details, see [Managing Gateway Servers in Operations Manager 2012](#).

If you deploy an agent in one of these locations, you will also need to request and configure a certificate that enables the watcher node to send alerts to System Center Operations Manager. To simplify this process, the Operations Manager team has created a set of utilities that enable you to request and install the correct type of certificate on the watcher node computer. For details, and to download these utilities, see [Obtaining Certificates for Non-Domain Joined Agents Made Easy with Certificate Generation Wizard](#).

### Installing the Operation Manager Agent Files

1. On your System Center setup media, double-click **Setup.exe**.
2. In the System Center Operation Manager setup wizard, click **Install Operations Manager Agent**, from Install Agent under Optional Installations
3. In the System Center setup wizard, on the Welcome to the System Center Operations Manager Setup wizard page, click **Next**.
4. On the Destination Folder page, select the folder where the Operations Manager Agent files will be installed and click **Next**.
5. On the Management Group Configuration page, select **Specify Management Group information** and click **Next**.
6. On the Management Group Configuration page, type the name of your Operations Manager Management Group in the **Management Group Name** box, and then type the host name of your Operations Manager server (for example, atl-scom-001) in the **Management Server** box. If you changed the port number used by Operations Manager, enter the new port number in the **Management Server Port** box. Otherwise, leave the port at the default value of 5723, and then click **Next**.
7. On the Agent Action Account page, select **Local System** and click **Next**.
8. On the Microsoft Update page, select **I don't want to use Microsoft Update** and click **Next**.

9. On the Ready to Install page, click **Install**.
10. On the Completing the System Center Operations Manager Setup wizard page, click **Finish**.
11. Click **Exit**.

For System Center 2012, you can verify that the agent has been created by clicking **Start**, clicking **All Programs**, clicking **System Center Operations Manager 2012**, and then clicking **Operations 2012 Manager Shell**. In the Operations Manager Shell, type the following Windows PowerShell command, and then press ENTER:

```
Get-SCOMAgent
```

A list of all your Operations Manager agents will appear.

## Configuring the Skype for Business Server Computer to Participate in System Center Discovery

To make sure that your new Skype for Business Server agent participates in the discovery process for System Center Operations Manager, you must complete the following procedure on each computer where the System Center Operations Manager console has been installed:

1. On the Administration tab, click **Agent Managed**.
2. Click on **Discovery Wizard** and complete the wizard for the computer to be discovered.
3. Reboot the Health Agent service. Rebooting the service will force discovery of the new machine. If you do not reboot the service, it could take as long as 4 hours before the new machine is discovered by System Center Operations Manager.
4. Verify that no error events were recorded in the Operations Manager event log.
5. The computer where the agent is pushed successfully will be shown under "Agent Managed" list and the computer where agent was installed manually will be shown under "Pending Management", click on the computer name and approve.
6. Right-click the name of the computer, and then click **Properties**. In the Properties dialog box, on the Security tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**, and then click **OK**.

# Configure watcher node test users and settings

5/20/2019 • 15 minutes to read

**Summary:** Configure test user accounts and watcher node settings for Skype for Business Server synthetic transactions.

After configuring the computer that will act as a watcher node, you must:

1. [Configure Test User Accounts](#) to be used by these watcher nodes. If you are using the Negotiate authentication method, you must also use the **Set-CsTestUserCredential** cmdlet to enable these test accounts for use on the watcher node.
2. Update the watcher node configuration settings.

## Configure Test User Accounts

Test accounts do not need to represent actual people, but they must be valid Active Directory accounts. In addition, these accounts must be enabled for Skype for Business Server, they must have valid SIP addresses, and they should be enabled for Enterprise Voice (to use the Test-CsPstnPeerToPeerCall synthetic transaction).

If you are using the TrustedServer authentication method, all you need to do is to make sure that these accounts exist and configure them as noted. You should assign at least three test users for each pool that you want to test. If you are using the Negotiate authentication method, you must also use the Set-CsTestUserCredential cmdlet and the Skype for Business Server Management Shell to enable these test accounts to work with the synthetic transactions. Do this by running a command similar to the following (these commands assume that the three Active Directory user accounts have been created and that these accounts are enabled for Skype for Business Server):

```
Set-CsTestUserCredential -SipAddress "sip:watcher1@litwareinc.com" -UserName "litwareinc\watcher1" -Password "P@ssw0rd"
Set-CsTestUserCredential -SipAddress "sip:watcher2@litwareinc.com" -UserName "litwareinc\watcher2" -Password "P@ssw0rd"
Set-CsTestUserCredential -SipAddress "sip:watcher3@litwareinc.com" -UserName "litwareinc\watcher3" -Password "P@ssw0rd"
```

You must include not only the SIP address, but also the user name and password. If you do not include the password, the Set-CsTestUserCredential cmdlet will prompt you to enter that information. The user name can be specified by using the domain name\user name format shown in the preceding code block.

To verify that the test user credentials were created, run these commands from the Skype for Business Server Management Shell:

```
Get-CsTestUserCredential -SipAddress "sip:watcher1@litwareinc.com"
Get-CsTestUserCredential -SipAddress "sip:watcher2@litwareinc.com"
Get-CsTestUserCredential -SipAddress "sip:watcher3@litwareinc.com"
```

Information similar to this will be returned for each user:

USERNAME	PASSWORD
Litwareinc\watcher1	System.Security.SecureString

## Configure a Basic Watcher Node with the Default Synthetic Transactions

After the test users have been created, you can create a watcher node by using a command similar to this:

```
New-CsWatcherNodeConfiguration -TargetFqdn "atl-cs-001.litwareinc.com" -PortNumber 5061 -TestUsers @{Add="sip:watcher1@litwareinc.com","sip:watcher2@litwareinc.com","sip:watcher3@litwareinc.com"}
```

This command creates a new watcher node that uses the default settings and runs the default set of synthetic transactions. The new watcher node also uses the test users `watcher1@litwareinc.com`, `watcher2@litwareinc.com`, and `watcher3@litwareinc.com`. If the watcher node uses TrustedServer authentication, the three test accounts can be any valid user accounts enabled for Active Directory and Skype for Business Server. If the watcher node uses the Negotiate authentication method, these user accounts must also be enabled for the watcher node by using the `Set-CsTestUserCredential` cmdlet.

To validate that automatic discovery of target pool to sign-in is configured correctly rather than targeting a pool directly use these steps instead:

```
New-CsWatcherNodeConfiguration -UseAutoDiscovery $true -TargetFqdn "atl-cs-001.litwareinc.com" -PortNumber 5061 -TestUsers @{Add="sip:watcher1@litwareinc.com","sip:watcher2@litwareinc.com","sip:watcher3@litwareinc.com"}
```

## Configuring Extended Tests

If you want to enable the PSTN test, which verifies connectivity with the public switched telephone network, you need to do some additional configuration when setting up the watcher node. First, you must associate your test users with the PSTN test type by running a command similar to this from the Skype for Business Server Management Shell:

```
$pstnTest = New-CsExtendedTest -TestUsers "sip:watcher1@litwareinc.com", "sip:watcher2@litwareinc.com", "sip:watcher3@litwareinc.com" -Name "Contoso Provider Test" -TestType PSTN
```

### NOTE

The results of this command must be stored in a variable. In this example, the variable is named `$pstnTest`.

Next, you can use the **New-CsWatcherNodeConfiguration** cmdlet to associate the test type (stored in the variable `$pstnTest`) to a Skype for Business Server pool. For example, the following command creates a new watcher node configuration for the pool `atl-cs-001.litwareinc.com`, adding the three test users created previously, and adding the PSTN test type:

```
New-CsWatcherNodeConfiguration -TargetFqdn "atl-cs-001.litwareinc.com" -PortNumber 5061 -TestUsers @{Add="sip:watcher1@litwareinc.com","sip:watcher2@litwareinc.com","sip:watcher3@litwareinc.com"} -ExtendedTests @{Add=$pstnTest}
```

The preceding command will fail if you have not installed the Skype for Business Server core files and the RTCLocal database on the watcher node computer.

To test multiple voice policies, you can create an extended test for each policy by using the **New-CsExtendedTest** cmdlet. The users provided should be configured with the desired voice policies. The extended tests are passed to the **New-CsWatcherNodeConfiguration** cmdlet by using comma-delimiters, such as:

```
-ExtendedTests @{Add=$pstnTest1,$pstnTest2,$pstnTest3}
```

Because the **New-CsWatcherNodeConfiguration** cmdlet was called without using the `Tests` parameter, only the Default synthetic transactions (and the specified extended synthetic transaction) will be enabled for the new

watcher node. Therefore, the watcher node will test the following components:

- Registration
- IM
- GroupIM
- P2PAV (peer-to-peer audio/video sessions)
- AvConference (audio/conferencing)
- Presence
- ABS (Address Book service)
- ABWQ (Address Book web service)

The following components will not be tested by default:

- ASConference
- AVEdgeConnectivity
- DataConference
- DialinConferencing
- ExumConnectivity (Exchange Unified Messaging)
- JoinLauncher
- MCXP2PIM (legacy mobile device instant messaging)
- P2PVideoInteropServerSipTrunkAV
- PersistentChatMessage
- PSTN (PSTN gateway calls, specified as an extended test)
- UcwaConference
- UnifiedContactStore
- XmppIM

### **Adding and Removing Synthetic Transactions**

After a watcher node has been configured, you can use the `Set-CsWatcherNodeConfiguration` cmdlet to add or remove synthetic transactions from the node. For example, to add the `PersistentChatMessage` test to the watcher node, use the `Add` method and a command similar to this:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Add="PersistentChatMessage"}
```

Multiple tests can be added by separating the test names by using commas. For example:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests  
@{Add="PersistentChatMessage","DataConference","UnifiedContactStore"}
```

An error will occur if one or more of these tests (for example, `DataConference`) has already been enabled on the watcher node. In this case, you will receive an error message similar to the following:

`Set-CsWatcherNodeConfiguration` : There is a duplicate key sequence 'DataConference' for the

'urn:schema:Microsoft.Rtc.Management.Settings.WatcherNode.2010:TestName' key or unique identity constraint.

When this error occurs, no changes will be applied. The command should be re-run with the duplicate test removed.

To remove a synthetic transaction from a watcher node, use the Remove method. For example, this command removes the ABWQ test from a watcher node:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Remove="ABWQ"}
```

You can use the Replace method to replace all the currently-enabled tests with one or more new tests. For example, if you want a watcher node only to run the IM test, you can configure that by using this command:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Replace="IM"}
```

When you run this command, all synthetic transactions on the specified watcher node will be disabled except for IM.

### Viewing and Testing the Watcher Node Configuration

If you want to view the tests that have been assigned to a watcher node, use a command similar to this:

```
Get-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" | Select-Object -ExpandProperty Tests
```

This command will return information similar to this, depending on the synthetic transactions that have been assigned to the node:

Registration IM GroupIM P2PAV AvConference Presence PersistentChatMessage DataConference

#### TIP

To view the synthetic transactions in alphabetical order, use this command instead:

```
Get-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" | Select-Object -ExpandProperty Tests | Sort-Object
```

To verify that a watcher node has been created, type the following command from the Skype for Business Server Management Shell:

```
Get-CsWatcherNodeConfiguration
```

You will get back information similar to this:

```
Identity : atl-cs-001.litwareinc.com TestUsers : {sip:watcher1@litwareinc.com, sip:watcher2@litwareinc.com ...}
ExtendedTests : {TestUsers=IList<System.String>;Name=PSTN Test; Te...} TargetFqdn : atl-cs-001.litwareinc.com
PortNumber : 5061
```

To verify that the watcher node has been configured correctly, type the following command from the Skype for Business Server Management Shell:

```
Test-CsWatcherNodeConfiguration
```

This command will test each watcher node in your deployment and confirm whether the following actions are completed:



- The required Registrar role is installed
- The required registry key is created (completed when you ran the Set-CsWatcherNodeConfiguration cmdlet)
- Your servers are running the correct version of Skype for Business Server
- Your ports are configured correctly
- Your assigned test users have the required credentials

## Managing Watcher Nodes

In addition to modifying the synthetic transactions that are executed on a watcher node, you can also use the **Set-CsWatcherNodeConfiguration** cmdlet to carry out two other important tasks: enabling and disabling the watcher node, and configuring the watcher node to use either internal Web URLs or external Web URLs when running its tests.

By default, watcher nodes are designed to periodically run all their enabled synthetic transactions. At times, however, you may want to suspend those transactions. For example, if the watcher node is temporarily disconnected from the network, then there is no reason to run the synthetic transactions. Without network connectivity, those transactions will fail. To temporarily disable a watcher node, run a command similar to this from the Skype for Business Server Management Shell:

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -Enabled $False
```

This command will disable the execution of synthetic transactions on the watcher node atl watcher 001.litwareinc.com. To resume execution of the synthetic transactions, set the Enabled property back to True (\$True):

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -Enabled $True
```

### NOTE

The Enabled property can be used to turn watcher nodes on or off. If you want to permanently delete a watcher node, use the **Remove-CsWatcherNodeConfiguration** cmdlet:

```
Remove-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com"
```

That command removes all the watcher node configuration settings from the specified computer, which prevents that computer from automatically running synthetic transactions. However, the command does not uninstall the System Center agent files or the Skype for Business Server system files.

By default, watcher nodes use an organization's external Web URLs when conducting tests. However, watcher nodes can also be configured to use the organization's internal Web URLs. This enables administrators to verify URL access for users located inside the perimeter network. To configure a watcher node to use internal URLs instead of external URLs, set the UseInternalWebURLs property to True (\$True):

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -UseInternalWebURLs $True
```

Resetting this property to the default value of False (\$False) will cause the watcher to once again use the external URLs:

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -UseInternalWebUrls $False
```

## Special Setup Instructions for Synthetic Transactions

Most synthetic transactions can run on a watcher node as-is. In most cases, as soon as the synthetic transaction is added to the watcher node configuration settings, the watcher node can begin using that synthetic transaction during its test passes. However, there are some synthetic transactions that require special setup instructions, as discussed in the following sections.

### Data Conferencing Synthetic Transaction

If your watcher node computer is located outside your perimeter network, you will probably not be able to run the Data Conferencing Synthetic Transaction unless you first disable the Windows Internet Explorer® Internet browser proxy settings for the Network Service account by completing the following steps:

1. On the watcher node computer, click **Start**, click **All Programs**, click **Accessories**, right click **Command Prompt**, and then click **Run as administrator**.
2. In the console window, type the following command and then press ENTER.

```
bitsadmin /util /SetIEProxy NetworkService NO_PROXY
```

You will see the following message displayed in the command window:

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows. Administration tools for the BITS service are now provided by BITS PowerShell cmdlets.

Internet proxy settings for account NetworkService set to NO\_PROXY.

(connection = default)

This message indicates that you have disabled the Internet Explorer proxy settings for the Network Service account.

### Exchange Unified Messaging Synthetic Transaction

The Exchange Unified Messaging (UM) synthetic transaction verifies that test users can connect to voicemail accounts homed in Exchange.

The test users will need to be preconfigured with voicemail accounts.

### Persistent Chat Synthetic Transaction

To use the Persistent Chat synthetic transaction, you must first create a channel and give the test users permissions to use it.

You can use the Persistent Chat synthetic transaction to configure this channel:

```
$cred1 = Get-Credential "contoso\testUser1"
$cred2 = Get-Credential "contoso\testUser2"

Test-CsPersistentChatMessage -TargetFqdn pool0.contoso.com -SenderSipAddress sip:testUser1@contoso.com -
SenderCredential $cred1 -ReceiverSipAddress sip:testUser2@contoso.com -ReceiverCredential $cred2 -
TestUser1SipAddress sip:testUser1@contoso.com -TestUser2SipAddress sip:testUser2@contoso.com -Setup $true
```

You must run this setup task must be run from inside the enterprise:

- If run from a non-server machine, the user who executes the cmdlet must be a member of the CsPersistentChatAdministrators role for Role-Based Access Control (RBAC).

- If run from the server itself, the user who executes the cmdlet must be a member of the RTCUniversalServerAdmins group.

### **PSTN Peer-to-Peer Call Synthetic Transaction**

The Test-CsPstnPeerToPeerCall synthetic transaction verifies the ability to place and receive calls through a public switched telephone network (PSTN).

To run this synthetic transaction, you must configure:

- Two UC-enabled test users (a caller and a receiver).
- Direct Inward Dialing (DID) numbers for each user account.
- VoIP Policies and Voice routes that allow calls to the receiver's number to reach the PSTN gateway.
- A PSTN gateway that accepts call and media that will route calls back to a receiver's home pool, based on the number dialed.

### **Unified Contact Store Synthetic Transaction**

The Unified Contact Store synthetic transaction verifies the ability of Skype for Business Server to retrieve contacts on behalf of a user from Exchange.

To use this synthetic transaction, the following conditions must be met:

- Lyss-Exchange server to server authentication must be configured.
- Test users must have a valid Exchange mailbox.

After these conditions are met, you can run the following Windows PowerShell cmdlet to migrate the test users' contact lists to Exchange:

```
Test-CsUnifiedContactStore -TargetFqdn pool0.contoso.com -UserSipAddress sip:testUser1@contoso.com -RegistrarPort 5061 -Authentication TrustedServer -Setup
```

It may take some time for the test user contact lists to migrate to Exchange. To monitor the migration progress, the same command-line can be run without the -Setup flag:

```
Test-CsUnifiedContactStore -TargetFqdn pool0.contoso.com -UserSipAddress sip:testUser1@contoso.com -RegistrarPort 5061 -Authentication TrustedServer
```

This command line will succeed after migration is completed.

### **XMPP Synthetic Transaction**

The Extensible Messaging and Presence Protocol (XMPP) IM synthetic transaction requires that you configure the XMPP feature with one or more federated domains.

To enable the XMPP synthetic transaction, you must provide an XmppTestReceiverMailAddress parameter with a user account at a routable XMPP domain. For example:

```
Set-CsWatcherNodeConfiguration -Identity pool0.contoso.com -Tests @{Add="XmppIM"} -XmppTestReceiverMailAddress user1@litwareinc.com
```

In this example, a Skype for Business Server rule will need to exist to route messages for litwareinc.com to an XMPP gateway.

#### NOTE

XMPP Gateways and proxies were available in Skype for Business Server 2015 but are no longer supported in Skype for Business Server 2019. See [Migrating XMPP federation](#) for more information.

### Video Interop Server (VIS) Synthetic Transaction

The Video Interop Server (VIS) synthetic transaction requires that you download and install the synthetic transaction support files ([VISSTSupportPackage.msi](#)).

To install VISSTSupportPackage.msi ensure the dependencies (under System Requirements) for the msi are already installed. Run VISSTSupportPackage.msi to do a simple installation. The .msi installs all the files in the following path: "%ProgramFiles%\VIS Synthetic Transaction Support Package".

For more details on how to run the VIS Synthetic Transaction refer to the documentation for the [Test-CsP2PVideoInteropServerSipTrunkAV](#) cmdlet.

## Changing the Run Frequency for Synthetic Transactions

By default, synthetic transactions will run with the configured users every 15 minutes. Synthetic transactions are run sequentially within a set of users to avoid two synthetic transactions from conflicting with each other. A longer interval is needed to provide time for all synthetic transactions to complete.

If it is desirable to run synthetic transactions more frequently, the number of synthetic transactions run with a given set of users should be decreased so that the tests can complete in the desired time range with some buffer for occasional network delays. If running more synthetic transactions is desirable, create more user sets to run additional synthetic transactions.

To change the frequency at which synthetic transactions run, follow these steps:

1. Open System Center Operations Manager. Click Authoring section. Click Rules section (under Authoring)
2. In the Rules section, find the rule with the name "Main Synthetic Transaction Runner Performance Collection Rule"
3. Right click the rule, and select Overrides, select Override the Rule, and then select "For All objects of class: Pool Watcher"
4. In the Override Properties window, select Parameter Name "Frequency", and set the Override Value to the desired one.
5. In the same window, select the Management pack to which this override needs to be applied

## Using Rich Logging for Synthetic Transactions

Synthetic transactions prove extremely useful in helping to identify issues with the system. For example, the Test-CsRegistration cmdlet could alert administrators to the fact that users were having difficulty registering with Skype for Business Server. However, additional details may be needed to determine the actual cause of a failure.

For this reason, synthetic transactions provide rich logging. With rich logging, for each activity that a synthetic transaction undertakes, the following information is recorded:

- The time that the activity started.
- The time that the activity finished.
- The action that was performed (for example, creating, joining, or leaving a conference; signing on to Skype for Business Server; sending an instant message).

- Informational, verbose, warning, or error messages generated when the activity ran
- SIP registration messages.
- Exception records or diagnostic codes generated when the activity ran.
- The net result of running the activity.

This information is automatically generated each time a synthetic transaction is run, but is not automatically displayed or saved to a log file. If you are manually running a synthetic transaction, you can use the `OutLoggerVariable` parameter to specify a Windows PowerShell variable in which the information will be stored. From there, you have the option of using one of two methods to save and/or view error messages in the rich log in either XML or HTML format.

To retrieve the troubleshooting information, specify the `OutLoggerVariable` parameter, followed by a variable name that you choose:

```
Test-CsRegistration -TargetFqdn atl-cs-001.litwareinc.com -OutLoggerVariable RegistrationTest
```

#### NOTE

: Do not preface the variable name with the `$` character. Use a variable name such as `RegistrationTest` (not `$RegistrationTest`).

When you run this command, you will see output similar to this:

Target Fqdn : atl-cs-001.litwareinc.com Result : Failure Latency : 00:00:00 Error Message : This machine does not have any assigned certificates. Diagnosis :You can access much more detailed information for this failure than just the error message shown here. To access this information in HTML format, use a command similar to this one to save the information stored in the variable `RegistrationTest` to an HTML file:

```
$RegistrationTest.ToHTML() | Out-File C:\Logs\Registration.html
```

Alternatively, you can use the `ToXML()` method to save the data to an XML file:

```
$RegistrationTest.ToXML() | Out-File C:\Logs\Registration.xml
```

You can view these files by using Windows Internet Explorer, Microsoft Visual Studio, or any other application capable of opening HTML/XML files.

Synthetic transactions run from inside of System Center Operations Manager will automatically generate these log files for failures. These logs will not be generated if the execution fails before Skype for Business Server PowerShell is able to load and run the synthetic transaction.

#### IMPORTANT

By default, Skype for Business Server saves log files to a folder that is not shared. To make these logs readily accessible, you should share this folder. For example: `\atl-watcher-001.litwareinc.com\WatcherNode`.

# Skype for Business Server Capacity Planning Calculator

5/20/2019 • 6 minutes to read

**Summary:** How to use the Capacity Calculator Tool.

## NOTE

This article references Skype for Business Server 2015 downloads, but it applies to:

- Skype for Business Server 2019.
- Skype for Business Server 2015.

The [Skype for Business Server 2015 Capacity Calculator](#) and [Skype for Business Server 2019 Capacity Calculator](#) augment the [Skype for Business Planning Tool](#) and your deployment documentation ([Plan for your Skype for Business Server 2015 deployment](#) and [Plan for your Skype for Business Server 2019 deployment](#) respectively). Use the calculator after you have reviewed the guide and created a recommended topology by using the Planning Tool.

The Skype for Business Server Capacity Calculator helps you determine server requirements based on the number of users and the communication tools your organization uses. After you have determined your user profile and the functions you want to enable for your users, use the calculator to determine the number of servers, memory, and bandwidth you will need. This version of the calculator does not provide guidance for disk I/O requirements.

You can benefit most from the calculator if you have accurate, detailed information about your specific user profile. For example, the percentage of voice-enabled users, average calls per user per hour, call duration, and the percentage of concurrent users in conferences can make a huge difference in server requirements. The accuracy of the recommendations created by the calculator depends on the accuracy of the information that you provide.

Once you have used the Planning Tool and the Capacity Planning Calculator, you should simulate your proposed and planned load to ensure that Skype for Business Server will be adequately provisioned. To perform stress testing under a simulated load, use the [Skype for Business Server Stress and Performance Tool](#) documented at [Skype for Business Server Stress and Performance Tool](#).

## Using the Capacity Calculator

The calculator is a Microsoft Excel spreadsheet. Your input cells are colored orange. Default values are entered in the cells (For Skype for Business Server 2015, 80,000 users in one pool with twelve Front End Servers, while for Skype for Business Server 2019, 106,000 users in one pool with sixteen Front End Servers), but you should change these values to match your organization's needs.

The usage model contains the following sections. To calculate your capacity requirements, enter data as described starting at the top of the sheet and working down row by row:

### Instant Messaging and Presence

- Under **Number of Users**, type the number of users who will be signed in at once. This number is typically 80% of the total number of provisioned users. In most situations, 100% of your concurrent users will be enabled for IM and Presence. The default is 80,000 for Skype for Business Server 2015, and 106,000 users for Skype for Business Server 2019.

- **Average number of contacts in Contact list** indicates the number of contacts that we are using to validate your system requirements. This number is fixed and not something you should change.

### Enterprise Voice

- In **Users enabled for Enterprise Voice**, type the percentage of your users enabled for Enterprise Voice. The default is 60%.
- In **Average number of calls per user per hour (peak)**, type the number of calls per hour you expect the average user to participate in during times of peak load. The default is 4.
- In **Percentage of calls that use media bypass**, type the percentage of calls placed by your users that will bypass the Mediation Server. The default is 65%, but could be lower if you are spread out geographically or have a large percentage of users who work from home.
- In **Percentage of voice users involved in UC-PSTN calls**, type the percentage of your organization's calls which are UC-PSTN phone calls. The default is 60%.
- **Percentage of voice users involved in UC-UC calls** shows the percentage of users who are enabled for Enterprise Voice who will be enabled only for UC-UC calls. This number is calculated based on what you input for **Percentage of voice users enabled for UC-PSTN calls**.

### Conferencing

- In **Percentage of users in concurrent conferences**, type the percentage of users who will be participating in conferences at the same time. The default is 5%.
- In **Percentage of conferences with group IM only (no voice)**, type the percentage of conferences that will involve instant messaging only and do not include audio. The default is 10%.
- In **Percentage of users using dial-in conferencing**, type the percentage of participants in conferences who will be using dial-in conferencing at one time. The default is 15%.
- In **Percentage of conferences using voice**, type the percentage of conferences that will include audio.
  - If 20% of your voice conferences will also include regular video, select the **Including video (no Multi View)** check box.
  - If 20% of your conferences will also include Multi-View video, select the **Including Multi View** check box.
  - If 50% of your voice conferences will also include application sharing, select the **Including application sharing** check box.
  - If 20% of your voice conferences include data uploads, such as PowerPoint presentations, select the **Including web conferencing** check box.

### Mobility

- In **Percentage of users enabled for Mobility**, type the percentage of your users who will be enabled to connect to Skype for Business Server using mobile devices. The default is 40%.

When you have entered all the necessary information, the capacity calculator estimates your requirements. The yellow cells show calculated values for CPU, memory, and bandwidth requirements based on tests performed in Skype for Business Server performance labs. The numbers are provided as a guideline, not every single variation is tested and validated. The following values are calculated:

- **Front End CPU**: Percentage of CPU usage if the entire load were being handled by one Front End Server of the same specifications as the server that was used in testing (see the description at the end of this article).
- **Network in Mbps**: Bandwidth requirements in megabits per second (Mbps) for the corresponding

workload.

- **Memory in GB:** Memory required in gigabytes (GB) for the corresponding workload.

The green cells show recommendations for the usage model that you entered.

- **Total Front End Servers:** The number of physical servers required are based on dedicated servers running Skype for Business Server 2015 with dual processor, hex-core, with 2,260 megacycles, or Skype for Business Server 2019 with Intel Xeon E5-2673 v3, dual processor, hex-core.

Note that enabling hyperthreading is recommended and has been proven to improve performance for servers that support audio/video.

- **Edge Servers:** The number of Edge Servers required, based on 30% of all concurrent users communicating through the Edge Servers. This percentage cannot be changed in the calculator.
- **Archiving/Call Detail Recording/Quality of Experience services Store:** The number of stores required for Archiving or Monitoring features, if they are enabled in your organization.
- **Back End Database Server Required (Pools Required):** The number of back-end database servers required to support the selected workload.

Additionally, in the row next to Total Front End Servers, more information is provided about the load on your servers and network for all the planned workloads combined.

- **Average CPU Load:** The average CPU usage per Front End server.
- **Network in Mbps:** The required bandwidth allocation to support the usage model that you entered.
- **Memory in GB:** Memory, in gigabytes, required for each Front End server.

### Adjusting For Your Processors

All the CPU usage figures in the spreadsheet assume that each Skype for Business Server 2015 server has a dual processor, hex-core with 2.26 GHz, at least 32 GB of memory, and 8 or more 10,000-RPM hard disk drives with at least 72 GB free disk space. For each Skype for Business Server 2019 server, all the CPU usage figures in the spreadsheet assume that each server has a dual processor, hex-core with Intel Xeon E5-2673 v3, at least 64 GB of memory, and 8 or more 10,000-RPM hard disk drives with at least 72 GB free disk space.

If your servers have different processors, you can adjust the figures to match your hardware.