Cisco Webex Meetings Enterprise Deployment Guide for Video Device-Enabled Meetings

First Published: 2015-09-23

Last Modified: 2020-01-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Deployment Options** 1

About Video Device-Enabled Cisco Webex Meetings 1

Example: SIP Site with Cisco Infrastructure 1

Example: SIP Site and Microsoft Skype for Business (or Lync) Site 2

Example: SIP and Microsoft Skype for Business (or Lync) Together in One Site 3

Security Options 3

CHAPTER 2 **Requirements and Recommendations** 5

System Requirements 5

Network Infrastructure 7

Video Devices 7

Microsoft Skype for Business (or Lync) Interoperability 9

Supported Environments 9

Supported Clients 9

H.323 Mode 9

CHAPTER 3 **Deployment Tasks** 11

Deployment Task Flow 11

Open the Port Range for the Cisco Webex Cloud 13

Short Video Address Format 13

Configure DNS Zone and Search Rule 13

Configure a Traversal Server/Client Pair 16

Route Video Call-Back Traffic 19

Reduce the Default SIP TCP Timeout on the Cisco Expressway-E 20

Enable BFCP for Presentation Sharing 21

Configure a SIP Trunk 22

Add a Route Pattern 22
Configure Bandwidth Controls 23
Simplify the Video Dial String 23
Configure Site Administration Settings 24
Configure Microsoft Skype for Business (or Lync) Federation 24
Deploy with CA-Signed Certificates 25
Generate Certificate Signing Request 27
Install the Signed SSL Server Certificate 27
Configure the Trusted CA List on the Cisco Expressway-E 27
Verify the Service 28

CHAPTER 4 Video Meetings 29
Using Both Cisco Collaboration Meeting Rooms Hybrid and Video Device-Enabled Cisco Webex Meetings Offerings Together 29
About TSP Audio 29

CHAPTER 5 Configure One Button to Push 31
One Button to Push 31
Configure Cisco TelePresence Management Suite Extension for Microsoft Exchange 31
Prerequisites 31
Deployment Best Practices 32
Configuring Cisco TMSXE for One Button to Push 32
Installing the Booking Service 32
Configuring IIS for HTTPS 32
Configuring the Server Certificate 33
Configuring the Location Displayed for TelePresence Rooms in Outlook 35
Adding Cisco TMS Managed Endpoints to Exchange 35

CHAPTER 6 Troubleshooting 37
Troubleshooting Problems with TSP Audio 37
Packet Loss on MPLS or Site-to-Site VPN Networks 37
Version Compatibility 38

CHAPTER 1

Deployment Options

- About Video Device-Enabled Cisco Webex Meetings, on page 1
- Example: SIP Site with Cisco Infrastructure, on page 1
- Example: SIP Site and Microsoft Skype for Business (or Lync) Site, on page 2
- Example: SIP and Microsoft Skype for Business (or Lync) Together in One Site, on page 3
- Security Options, on page 3

About Video Device-Enabled Cisco Webex Meetings

Participants can join a video meeting from the Cisco Webex Meetings web application, from a phone, or from a video device. Video devices negotiate all media (main video, content, and audio) to and from the Cisco Webex cloud. This media flows over IP negotiated by using SIP or H.323 (SIP is recommended). Cisco TelePresence infrastructure may be used for call control and firewall traversal, but is not required.

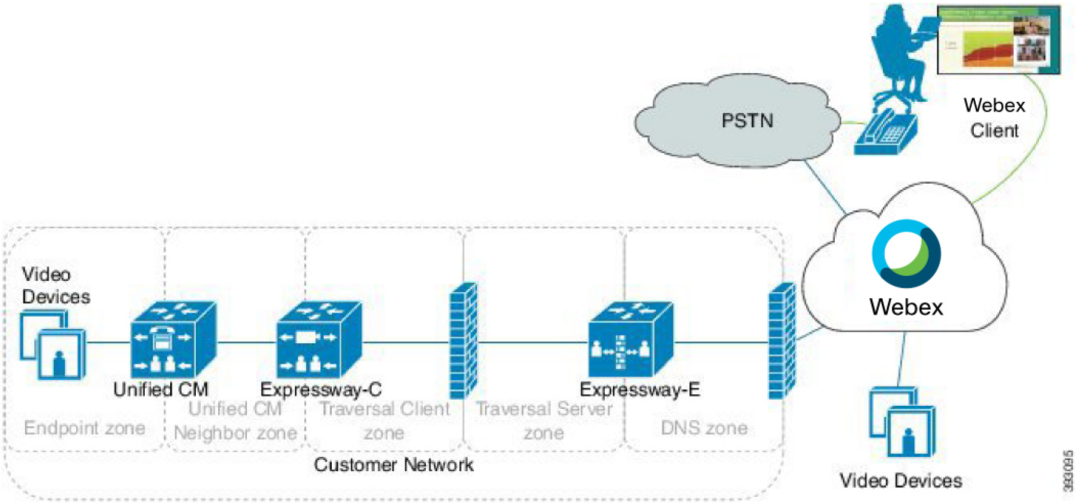
Cisco Webex offers multiple audio solution options for Cisco Webex Meetings application users and phone participants. For Cisco Webex Meetings with video, available options are Cisco Webex Audio (including Cloud Connected Audio) and Teleconferencing Service Provider (TSP) audio that has been verified compatible with Cisco Webex video platform/video conferencing.

Contact your Cisco Account Manager for more information about Cisco Webex Audio, and to obtain the latest list of verified TSP Audio Provider partners.

Example: SIP Site with Cisco Infrastructure

In this example, the enterprise video devices are registered to Unified Communications Manager, with Cisco Expressway-C and Cisco Expressway-E being used for secure calling and firewall traversal.

Figure 1: SIP Site Using Unified Communications Manager



Other deployments are also possible with Cisco TelePresence infrastructure, including:

- Cisco VCS Control and Cisco VCS Expressway

  Video devices are registered to Cisco VCS Control rather than to Unified Communications Manager.

- Cisco VCS Control and Cisco VCS Expressway with Unified Communications Manager

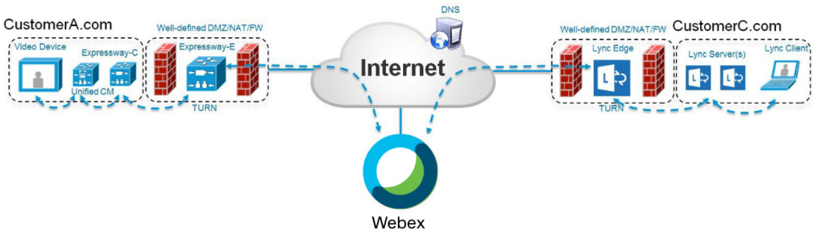
  Video are registered to Cisco VCS Control and Unified Communications Manager (a combination of the above two models).

Example: SIP Site and Microsoft Skype for Business (or Lync) Site

Microsoft Skpe for Business was previously know as Microsoft Lync. This document will refer to Skype for Business only for the most part.

In this example, attendees join a video meeting from two types of deployment. CustomerA uses SIP with Cisco infrastructure, including Unified Communications Manager for call control and Cisco Expressway for firewall/NAT traversal. CustomerC has no Cisco infrastructure equipment. The Skype for Business servers at CustomerC communicate directly with the Cisco Webex cloud.

Figure 2: SIP Site and Microsoft Skype for Business Site



Example: SIP and Microsoft Skype for Business (or Lync) Together in One Site

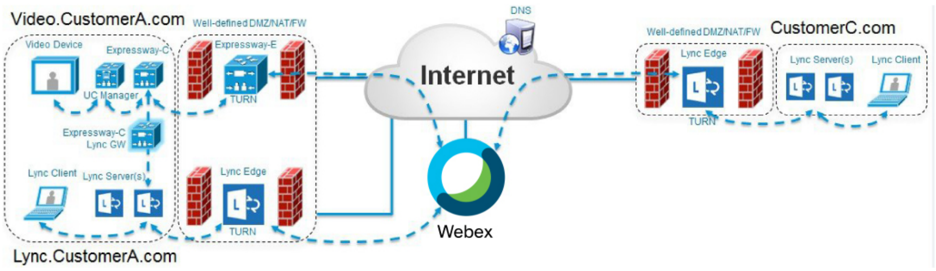
In this example, CustomerA has Cisco SIP infrastructure and video devices, as well as Skype for Business. CustomerC, as before, has no Cisco infrastructure equipment.

When a site combines Skype for Business and Cisco SIP clients, as in CustomerA's case, the following guidelines apply:

- The site should use both a Skype for Business Edge and an Expressway-E Edge.
- Skype for Business traffic destined for the Webex cloud should not be routed through the Expressway-C Lync gateway first.

  In the example, the Skype for Business servers for CustomerA would route traffic to video.customerA.com through the Expressway-C Lync gateway, but would route *.webex.com directly out via the Lync Edge.

Figure 3: SIP/Skype for Business Site and Microsoft Skype for Business Site



Security Options

For SIP calls, Video Device-Enabled Cisco Webex Meetings support any combination of certificate type, signaling, and media in the following table:

Certificates	Signaling	Media
• CA-signed certificates (recommended) • Self-signed certificates	• TLS • TCP	• sRTP (recommended) • RTP

By default, the Cisco Expressway (or Cisco VCS) uses self-signed certificates. For each SIP call, it attempts TLS signaling with fallback to TCP, and sRTP with fallback to RTP.

For H.323 calls, video device-enabled meetings support nonsecure H.225/H.245 signaling and H.235 media encryption methods.

For Skype for Business, video device-enabled meetings support TLS for signaling and sRTP for media.

CHAPTER 2

Requirements and Recommendations

- System Requirements, on page 5
- Network Infrastructure, on page 7
- Video Devices, on page 7
- Microsoft Skype for Business (or Lync) Interoperability, on page 9
- H.323 Mode, on page 9

System Requirements

Table 1: Requirements for Video Device-Enabled Cisco Webex Meetings Deployments

Requirement	Description
Cisco Webex Meetings	The Cisco Webex Meetings site must be running release WBS31 or later.
Audio	Cisco Webex offers multiple audio solution options for Cisco Webex application users and phone participants. For video device-enabled meetings, available options are Webex Audio (including Cloud Connected Audio) and Teleconferencing Service Provider (TSP) audio that has been verified compatible with Cisco Webex video platform/video device-enabled meetings. Contact your Cisco Account Manager for more information about Webex Audio, and to obtain the latest list of verified TSP Audio Provider partners.

Requirement	Description
Network access	Make sure that the port range for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls allows the following: • inbound media traffic from the Cisco Webex Cloud over UDP for the RTP port range 36000–59999 • inbound Skype for Business media traffic from Cisco Webex Cloud over TCP for the RDP port range 56000–57000 • inbound SIP signaling traffic from the Webex cloud over TCP for ports 5060, 5061, and 5065 • inbound H.323 signaling traffic from the Webex cloud over TCP port 1720 and port range 15000–19999 • outbound media traffic to the Webex cloud over UDP for the RTP port range 36000–59999 • outbound SIP signaling traffic to the Webex cloud over TCP for the ports 5060–5070 • outbound H.323 signaling traffic to the Webex cloud over TCP port 1720 and port range 15000–19999 For the IP address ranges used by the Webex cloud, by geographic location, see https://collaborationhelp.cisco.com/article/WBX264
Network bandwidth	The amount of network bandwidth that is required depends on the requirements of each video device to provide the desired video quality plus presentation data. We recommend at least 1.5 Mbps per screen for an optimal experience. Some video devices can take advantage of higher rates, and the service can accommodate lower rates, depending on the device.
Quality of service	The egress gateway must support the following DSCP markings: • Video traffic marked with DSCP AF41 as per RFC 2597 • Audio traffic marked with DSCP EF as per RFC 3246
One Button to Push (OBTP)	The following are required for OBTP: • TMS 15.2 and TMSXE 5.2 or later • A calendar management deployment compatible with Cisco TMS Exchange Extension 5.2 or later For more information on OBTP, see One Button to Push.

Network Infrastructure

You can use any standards-based call control system for your video devices. Your deployment may also include a firewall traversal device to provide mobile and remote access.

Note Cascading from an external conference bridge, for example on-premises MCU/TPS or third-party meeting, is not supported with Video Device-Enabled Cisco Webex Meetings due to the degraded user experience and feature limitations.

The following table lists recommended versions of Cisco products that can provide these functions. These components are not required.

Table 2: Recommended Network Infrastructure for Video Device-Enabled Cisco Webex Meetings Deployments

Component	Recommended Options from Cisco
Call control, device registration	• Cisco Unified Communications Manager (tested releases: 10.5, 9.1(2), and 9.1(1) • Cisco VCS Control and Cisco VCS Expressway (tested releases: X8.6)
Firewall traversal, mobile and remote access	• Cisco Expressway-C and Cisco Expressway-E (tested releases: X8.6) • Cisco VCS Control and Cisco VCS Expressway (tested release: X8.6) **Note** The minimum required version is X8.6.0 and the minimum recommended version is X8.6.1 (for free traversal/RMS calls to Webex with full URI dialing). We also recommend reducing the default SIP TCP timeout according to the deployment tasks for video device-enabled meetings. With versions prior to X8.6, callers can experience significant delays if the primary Webex call destination is unavailable. This happens because Cisco Expressway/Cisco VCS attempts to connect to each primary destination in the DNS SRV record in turn before it tries any backup destination, and in these versions, it applies a ten second SIP TCP timeout to every connection attempt.

Video Devices

The following table lists general requirements and considerations for each type of device.

Table 3: Video Device Requirements for Cisco Webex Meetings with Video Deployments

Type of Device or Client	Requirements
SIP	• In order for the participant to present or view shared content, the device must be able to negotiate Binary Floor Control Protocol (BFCP) with the cloud servers. Without BFCP, content cannot be shared and will be seen embedded in the main video channel. • In order for a device with three or more screens to display video on more than one screen, the device must be able to negotiate the TelePresence Interoperability Protocol (TIP) with the Webex cloud servers. **Note** SIP endpoints that are configured in standalone mode cannot join Webex meetings.
H.323	• H.323 devices must use URI dialing (Annex O) to call in to the Webex cloud. See your vendor-provided documentation for instructions on setting up URI dialing. • In order for the participant to present or view shared content, the device must be able to negotiate H.239 with the cloud servers. Without H.239, content cannot be shared and will be seen embedded in the video. • Multi-screen endpoints are not supported.
Microsoft Skype for Business	• Skype for Business clients that support the following video codecs (and resolutions) can join Webex meetings: • H.264-UC (720p30) • H.263 (CIF) • If the Short Video Address Format is enabled on your Webex site, Skype for Business users must dial a URI in the format <meetingID>@webex.com (for example, 123456789@webex.com) or <userID>.<sitename>@webex.com (for example, jdoe.customer-a@webex.com). If the short video address format isn't enabled on your Webex site, Skype for Business users must dial a Lync-specific URI in the format <meetingID>.<sitename>@lync.webex.com (for example, 123456789.customer-a@lync.webex.com) or <userID>.<sitename>@lync.webex.com (for example, jdoe.customer-a@lync.webex.com). • To start a meeting, Skype for Business users can enter the Host PIN, if the user is a meeting host. Likewise, to join a meeting before the host has started it, Skype for Business user can use the dial pad to enter # to enter the lobby. • Participants who joined from the Skype for Business application can share and view content in a Webex meeting.

Microsoft Skype for Business (or Lync) Interoperability

Microsoft Skype for Business support is provided as a feature, with some limitations, as described in the following sections. Cisco Webex reserves the right to disable the feature at any time without notice. Webex Technical Support will provide limited assistance to customers who attempt to use Skype for Business to join Webex meetings.

Note There will be feature limitations for mobile device support.

Supported Environments

- Lync 2013
- Skype for Business 2015
- Office 365

Supported Clients

For all the information on video compatibility and support, see http://cisco.com/go/cmr-cloud-compatibility

H.323 Mode

Video Device-Enabled Cisco Webex Meetings supports H.323. However, SIP has a richer feature set, support for secure signaling, and greater cloud capacity. We recommend turning off H.323 mode on the Cisco Expressway (or Cisco VCS). With H.323 mode off, Cisco Expressway interworks an H.323 endpoint's traffic into SIP and then sends a SIP invite to the Webex cloud.

CHAPTER 3

Deployment Tasks

- Deployment Task Flow, on page 11

Deployment Task Flow

Before you begin

When your Video Device-Enabled Cisco Webex Meetings order is complete, you will receive information about your Cisco Webex site access details (URLs and Site Administration account).

Procedure

	Command or Action	Purpose
Step 1	Open the Port Range for the Cisco Webex Cloud, on page 13	Set the port range for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls.
Step 2	Configure DNS Zone and Search Rule, on page 13	Configure the DNS zone and search rule if you want to ensure that TLS and sRTP are used in fallback scenarios (recommended).
Step 3	Configure a Traversal Server/Client Pair, on page 16	For secure calling, configure a Traversal Client zone and search rule on Cisco Expressway-C (or Cisco VCS Control) and a Traversal Server zone on Cisco Expressway-E (or Cisco VCS Expressway).
Step 4	Route Video Call-Back Traffic, on page 19	For video call-back, configure search rules on Cisco Expressway-C and Cisco Expressway-E (or Cisco VCS Control and Cisco VCS Expressway) to route Webex dial-outs to users' video devices.
Step 5	Reduce the Default SIP TCP Timeout on the Cisco Expressway-E, on page 20	Configure the SIP TCP timeout value on Cisco Expressway / Cisco VCS (X8.6) to the lowest value that is appropriate for your deployment.

	Command or Action	Purpose
Step 6	Enable BFCP for Presentation Sharing, on page 21	Verify that BFCP is enabled on the Unified Communications Manager neighbor zone in Cisco Expressway-C or Cisco VCS Control, and on the SIP profile in Unified Communications Manager.
Step 7	Configure a SIP Trunk, on page 22	Configure the SIP profile and trunk to Cisco Expressway-C (or Cisco VCS Control) on Unified Communications Manager in order for endpoints that are registered to Unified Communications Manager to participate in a video meeting and to call endpoints that are registered to a Cisco VCS Control.
Step 8	Add a Route Pattern, on page 22	Add a SIP route pattern in Unified Communications Manager for the webex.com domain.
Step 9	Configure Bandwidth Controls, on page 23	Configure your minimum desired bandwidth in Unified Communications Manager, and in Cisco Expressway or Cisco VCS.
Step 10	Simplify the Video Dial String, on page 23	Use pattern replacement to simplify the dial string for SIP and H.323 video devices within your enterprise.
Step 11	Configure Site Administration Settings, on page 24	Configure Webex site-wide and per-user settings for Cisco Webex Meetings with Video.
Step 12	Configure Microsoft Skype for Business (or Lync) Federation, on page 24	Enable Microsoft Skype for Business users to join your Webex meetings.
Step 13	Deploy with CA-Signed Certificates, on page 25	Complete the tasks in this section if you want to use CA-signed certificates to enable secure calling to the Webex cloud. These tasks require the Cisco Expressway Series (Cisco Expressway-C and Cisco Expressway-E) or Cisco VCS (Cisco VCS Control and Cisco VCS Expressway). To accomplish similar tasks on other vendors' equipment, refer to the vendor documentation.
Step 14	Verify the Service, on page 28	Test to ensure that your deployment of the Video Device-Enabled Cisco Webex Meetings service works correctly.

Open the Port Range for the Cisco Webex Cloud

This procedure specifies the port ranges that you must configure for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls. For detailed instructions, see Cisco Expressway Administrator Guide and Cisco VCS Administrator Guide.

Procedure

Use the management interface for your device to configure the following port ranges:

- inbound media traffic from the Webex cloud over UDP for the RTP port range 36000 – 59999
- inbound SIP signaling traffic from the Webex cloud over TCP for ports 5060 and 5061
- inbound H.323 signaling traffic from the Webex cloud over TCP port 1720 and port range 15000-19999
- outbound media traffic to the Webex cloud over UDP for the RTP port range 36000 – 59999
- outbound SIP signaling traffic to the Webex cloud over TCP for the ports 5060 – 5070
- outbound H.323 signaling traffic to the Webex cloud over TCP port 1720 and port range 15000-19999

Short Video Address Format

Users can now enter a shorter video address when they join a meeting from a video system. They can enter ***<meeting_number>*@webex.com** instead of the current video address format, **<meeting_number>@<site_name>.webex.com**. The existing video address format will continue to work.

The short video address feature isn't enabled by default. Webex administrators must enable short video address.

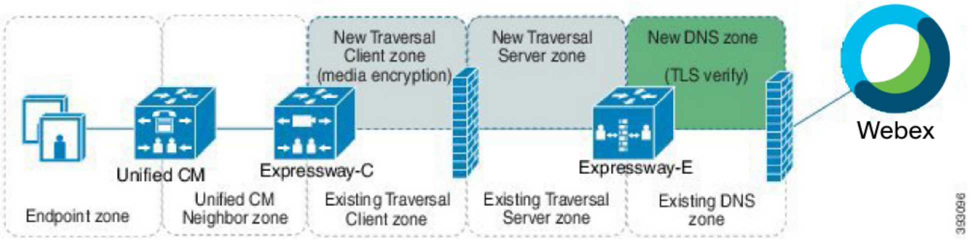
Before you begin

To use the new short video address format, create a search rule on both the Expressway-C and the Expressway-E. For more information, see Step 2 of Configure DNS Zone and Search Rule, on page 13 and Step 2 of Configure a Traversal Server/Client Pair, on page 16.

Configure DNS Zone and Search Rule

You can use the default DNS zone configuration on the Cisco Expressway-E (or Cisco VCS Expressway) to route calls to the Webex cloud. The default configuration will result in Cisco Expressway attempting best-effort TLS (with fallback to TCP) and sRTP media encryption (with fallback to RTP). However, we recommend the following zone configuration, especially if you want to ensure that TLS and sRTP are used.

Figure 4: Recommended DNS Zone Configuration for Encryption


New Traversal Client zone (media encryption)
New Traversal Server zone
New DNS zone
(TLS verify)
Webex
Unified CM
Expressway-C
Expressway-E
Endpoint zone
Unified CM Neighbor zone
Existing Traversal Client zone
Existing Traversal Server zone
Existing DNS zone
393096

Before you begin

We recommend turning off H.323 mode in this procedure. This forces Cisco Expressway to interwork an H.323 endpoint's traffic into SIP and then send a SIP invite to the Webex cloud.

Procedure

Step 1 Use the following table to configure the DNS zone on Cisco Expressway-E. The configuration varies depending on the type of certificate in use, and whether you turn on H.323 mode.

Zone Configuration Setting	Value if Using 3rd-Party CA Signed Certificate	Value if Using Self-Signed Certificate
H.323 Mode	**On** (default) or **Off** (recommended)	**On** (default) or **Off** (recommended)
SIP Media encryption mode	**Auto** (default)	**Auto** (default)
TLS Verify mode	**On**	**Off**
TLS verify subject name field	`sip.webex.com`	`sip.webex.com`
Advanced zone profile	**Default** or **Custom** (required if **H.323 Mode** is set to **Off**)	**Default** or **Custom** (required if **H.323 Mode** is set to **Off**)
Automatically respond to SIP searches	**Off** (default) or **On** (required if **H.323 Mode** is set to **Off**)	**Off** (default) or **On** (required if **H.323 Mode** is set to **Off)**
SIP SDP attribute line limit mode	**Off** (required if **Advanced zone profile** is set to **Custom**)	**Off** (required if **Advanced zone profile** is set to **Custom**)

Step 2 If the Short Video Address Format is enabled on your Webex site, create a search rule for the Webex domain on the Cisco Expressway-E, with the following properties. If you have an existing Webex dialing rule, make this new rule at the same priority value as the existing Webex dialing rule so that both dialing patterns work.

If the short video address format isn't enabled on your Webex site, got to Step 3.

Table 4: Expressway-E

Search Rule Setting	Value on Expressway-E
Priority	Use a lower numeric value than the search rule for any existing DNS zones.

Search Rule Setting	Value on Expressway-E
Protocol	**Any**
Source	<Admin Defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	`(.*)@(webex\.com).*`
Pattern Behavior	`Replace`
Replace String	`\1@\2`
On Successful Match	**Stop**
Target	<DNSzone used to route calls to the Webex cloud>
State	**Enabled**

Step 3 If the short video address format isn't enabled on your Webex site, create a search rule for the Webex domain on the Cisco Expressway-E, with the following properties:

Search Rule Setting	Value on Expressway-E
Priority	Use a lower numeric value than the search rule for any existing DNS zones.
Protocol	**Any**
Source	<Admin Defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	`(.*)@(.*)(\.webex\.com).*`
Pattern Behavior	`Replace`
Replace String	`\1@\2\3`
On Successful Match	**Stop**
Target	<DNS zone used to route calls to the Webex cloud>
State	**Enabled**

For detailed instructions, see the "Routing configuration" chapter of the applicable administration guide:

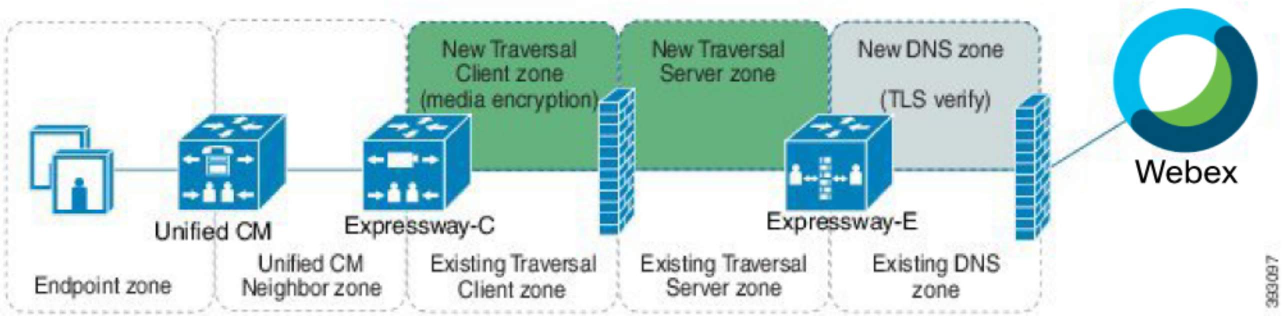
- Cisco Expressway Basic Configuration Deployment Guide
- Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide

Configure a Traversal Server/Client Pair

You can skip this task if you are happy with Cisco Expressway attempting best-effort TLS (with fallback to TCP) and sRTP media encryption (with fallback to RTP). In that case, the DNS zone configuration from the previous task is sufficient.

The recommended zone configuration for secure calling uses a Traversal Client zone on Cisco Expressway-C (or Cisco VCS Control) and a Traversal Server zone and DNS zone on Cisco Expressway-E (or Cisco VCS Expressway). If you already have one or more Traversal Client/Traversal Server zone pairs in your configuration, you can use these zones, but we recommend adding a new pair specifically for the Webex cloud.

Figure 5: Recommended Traversal Zone Pair Configuration for Encryption


New Traversal Client zone (media encryption)
New Traversal Server zone
New DNS zone
(TLS verify)
Webex
Unified CM
Expressway-C
Expressway-E
Endpoint zone
Unified CM Neighbor zone
Existing Traversal Client zone
Existing Traversal Server zone
Existing DNS zone
393097

In this procedure:

- On the Cisco Expressway-C, you apply the media encryption policy on the Traversal Client zone, and create a search rule that routes outbound Webex domain calls towards that zone.
- On the Cisco Expressway-E, you configure the TLS Verify mode on the DNS zone. (The search rule that routes outbound Webex domain calls towards that zone was configured in the previous task.)

We recommend this configuration for two reasons:

- To avoid unnecessarily engaging the B2BUA on the Cisco Expressway-E.
- To encrypt all traffic that egresses the firewall so that someone who may have access to your DMZ cannot sniff your traffic.

Procedure

Step 1 Use the following table to configure the Traversal Client and Traversal Server zones:

Zone Configuration Setting	Value On Traversal Client Zone (Cisco Expressway-C)	Value on Traversal Server Zone (Cisco Expressway-E)
H.323 Mode	**Off** (recommended) or **On** (default)	**Off** (recommended) or **On** (default)
SIP Media encryption mode	**Force Encrypted** or **Best Effort** (required if **H.323 Mode** is set to **On**)	**Auto**

Step 2 If the Short Video Address Format is enabled on your Webex site, create a search rule on the Cisco Expressway-C, with the following properties. If you have an existing Webex dialing rule, make this new rule at the same priority value as the existing Webex dialing rule so that both dialing patterns work.

If the short video address format hasn't been enabled on your Webex site, got to Step 3.

Table 5: Expressway-C

Search Rule Setting	Value on Expressway-C
Priority	Use a lower numeric value than any search rule that would match the webex.com domain (such as a default domain pattern string).
Protocol	**Any**
Source	<Admin Defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	`(.*)@(webex\.com).*`
Pattern Behavior	`Replace`
Replace String	`\1@\2`
On Successful Match	**Stop**
Target	<Traversal Client zone>
State	**Enabled**

Alternatively, if you would like to consolidate both of these search rules for both the old and the new format on your Expressway-C and the Expressway-E, use the format in the following tables:

Table 6: Expressway-C

Search Rule Setting	Value on Expressway-C
Priority	Use a lower numeric value than any search rule that would match the webex.com domain (such as a default domain pattern string).
Protocol	**Any**
Source	<Admin Defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	`(.*)@(webex\.com).*`
Pattern Behavior	`Replace`
Replace String	`\1@\2`

Search Rule Setting	Value on Expressway-C
On Successful Match	**Stop**
Target	<Traversal Client zone>
State	**Enabled**

Table 7: Expressway-E

Search Rule Setting	Value on Expressway-E
Priority	Use a lower numeric value than the search rule for any existing DNS zones.
Protocol	**Any**
Source	<Admin Defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	`(.*)@(.*webex\.com).*`
Pattern Behavior	`Replace`
Replace String	`\1@\2`
On Successful Match	**Stop**
Target	<DNSzone used to route calls to the Webex cloud>
State	**Enabled**

Step 3 If the short video address format isn't enabled on your Webex site, create a search rule on Cisco Expressway-C with the following properties:

Search Rule Setting	Value on Expressway-C
Priority	Use a lower numeric value than any search rule that would match the webex.com domain (such as a default domain pattern string).
Protocol	**Any**
Source	<Admin defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	`(.*)@(.*)(\.webex\.com).*`
Pattern Behavior	`Replace`
Replace String	`\1@\2\3`

Search Rule Setting	Value on Expressway-C
On Successful Match	**Stop**
Target	< Traversal Client zone>
State	**Enabled**

For additional information on zones and search rules, see the "Routing configuration" chapter of the applicable administration guide:

- Cisco Expressway Basic Configuration Deployment Guide
- Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide

Route Video Call-Back Traffic

Webex users can choose video call-back for an easier join experience, where the cloud calls the user's video directly. If you enable this for users, create search rules on the Expressway-E and Expressway-C to route these calls toward the users' home Cisco Unified Communications Manager cluster.

Procedure

Step 1 Go to **Configuration** > **Dial Plan** > **Search rules** and click **New**.

Create a rule on both systems. The method is the same but the rule values are different.

Step 2 Configure the search rules as follows:

	Cisco Expressway-C	Cisco Expressway-E
Rule name	"SIP callback from Webex toward internal call control" for example	"SIP callback from Webex toward Expressway-C" for example
Description	"Routes calls from traversal zone toward user home cluster" for example	"Matches Webex originated URIs, strips unnecessary parameters, and routes to traversal zone" for example
Priority	100	100
Protocol	SIP	SIP
Source	Named	Named
Source name	Traversal client zone <Admin defined name>	Default zone (This is where all calls come in from outside the organization's network)

	Cisco Expressway-C	**Cisco Expressway-E**
Request must be authenticated	No	No
Mode	Alias pattern match	Alias pattern match
Pattern type	Regex	Regex
Pattern string	.*@example\.com	(.*)@(example\.com);transport=[tlscp]{3}.* **Warning!** This pattern will match any string. Create a more specific string for your usernames and DNs, and your domains to prevent fraudulent calls. For example, if your DNs are all eight digits and start with the number 8, and your domain is contoso.com: ((8\d{7})|([A-Za-z].+))@(contoso\.com);transport=[tlscp]{3}.*
Pattern behavior	Leave	Replace
Replace string	N/A	\1@\2 Only keeps the username@FQDN portion, stripping off the transport and any other attributes or trailing characters.
On successful match	Stop	Stop
Target	<Admin defined>, select neighbor zone toward Cisco Unified Communications Manager	Traversal server zone, <Admin defined name>
State	Enabled	Enabled

Step 3 Click **Create search rule**.

Reduce the Default SIP TCP Timeout on the Cisco Expressway-E

From Cisco Expressway / Cisco VCS Version X8.6 the SIP TCP timeout value is configurable. The default value is 10 seconds. We strongly recommend that you set the timeout to the lowest value that is appropriate for your deployment. A value of 1 second is likely to be suitable in most cases, unless your network has extreme amounts of latency (such as video over satellite communications).

To set the SIP TCP timeout value:

Procedure

Step 1 Access the command line interface (this setting cannot be configured through the web interface).

Step 2 Type the following command, replacing "n" with the required timeout value:

```
xConfiguration SIP Advanced SipTcpConnectTimeout: n
```

Example: `xConfiguration SIP Advanced SipTcpConnectTimeout: 1`

Reducing the timeout is optional, but may improve performance in the event that the Cisco Expressway-E (or Cisco VCS Expressway) times out attempting to reach the primary Webex data center.

Enable BFCP for Presentation Sharing

This procedure specifies the BFCP settings that you must configure in the neighbor zone or SIP profile to enable presentation sharing. For detailed information about configuring zone profiles and SIP profiles, see the following documents:

- *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* for your version of Cisco Expressway, at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.
- *Cisco VCS and CUCM Deployment Guide* for your version of Cisco VCS, at http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html.

Note BFCP support was introduced in Cisco Unified Communications Manager version 8.6(1). We strongly recommend that you use a version no earlier than 8.6(2a)SU3 for BFCP interoperability.

Procedure

Step 1 Verify that BFCP is enabled on the Unified Communications Manager neighbor zone in Cisco Expressway-C or Cisco VCS Control:

- If you are using X8.1 or later, BFCP is automatically enabled when you choose the Cisco Unified Communications Manager (8.6.1 or later) zone profile on the Unified Communications Manager neighbor zone.
- If you are using a release prior to X8.1, set **SIP UDP/BFCP filter mode** to **Off** on the zone profile in Cisco VCS Control.

Step 2 Verify that BFCP is enabled on the SIP profile in Unified Communications Manager:

- If you are using X8.1 or later, BFCP is automatically enabled if you choose the **Standard SIP Profile for Cisco VCS** when defining the SIP trunk to the Cisco Expressway-C or Cisco VCS Control.
- If you are using a release prior to X8.1, check the **Allow Presentation Sharing using BFCP** box on the SIP profile.

Configure a SIP Trunk

Configure the SIP profile and trunk to Cisco Expressway-C (or Cisco VCS Control) on Unified Communications Manager in order for endpoints registered to Unified Communications Manager to participate in a video meeting and to call endpoints registered to a Cisco VCS Control.

This procedure provides high-level steps. For detailed instructions, see the following documents:

- *Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide* for your version of Cisco Expressway, at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.
- *Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide* for your version of http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html.

Procedure

Step 1 In Unified Communications Manager, configure a SIP trunk between Unified Communications Manager and Cisco Expressway-C (or Cisco VCS Control).

Step 2 Configure the SIP profile.

Step 3 To enable presentation sharing, check the **Allow Presentation Sharing using BFCP** check box in the **Trunk Specific Configuration** section of the **SIP Profile Configuration** window.

For third-party video devices that support BFCP, you may also need to check the **Allow Presentation Sharing using BFCP** check box in the **Protocol Specific Information** section of the **Phone Configuration** window.

Add a Route Pattern

Add a route pattern for the Webex domain in Unified Communications Manager.

Procedure

On the Unified Communications Manager, add a route pattern for *.webex.com (or *.*) and point it at the SIP trunk to Cisco Expressway-C (or Cisco VCS Control) .

For detailed instructions, see the applicable guide for your release:

- Unified Communications Manager release 11.0(1) and later: System Configuration Guide
- Earlier releases: Administration Guide

Configure Bandwidth Controls

Configure your minimum desired bandwidth in Unified Communications Manager, and in Cisco Expressway or Cisco VCS.

Procedure

Step 1 In Unified Communications Manager, set the region to permit the minimum desired bandwidth, to ensure optimum SIP audio and video connectivity between and the Webex cloud.

For detailed instructions, see "Regions" in the applicable guide for your release:

- Unified Communications Manager release 11.0(1) and later: System Configuration Guide
- Earlier releases: Administration Guide

Step 2 In Cisco Expressway or Cisco VCS, set zones and pipes appropriately (according to your network's requirements) to allow the minimum desired bandwidth.

For detailed instructions, see "Bandwidth control" in the applicable administrator guide:

- Cisco Expressway Administrator Guide
- Cisco VCS Administrator Guide

Simplify the Video Dial String

To join a scheduled video meeting, telepresence users typically must dial a string consisting of all digits in the meeting number followed by the @ symbol and webex.com—for example, a regular scheduled Webex meeting uses the following format:

12345678912@webex.com

Alternatively, personal rooms use the format of: username or other personalized alphanumeric 'dot' sitename followed by the @ symbol and webex.com. This is a sample personal room format for a Webex meeting on the 'sitename' Webex site:

example.sitename@webex.com

You can simplify this string for SIP and H.323 video devices within your enterprise by using pattern replacement. In this example, you add a short prefix that replaces the need for users to include the domain when dialing. In the example deployment, where enterprise video devices are registered to Unified Communications Manager and the Cisco Expressway Series (or Cisco VCS) is used for remote devices and firewall traversal, the simplified dial string is routed and converted into the full video dial string by a Unified Communications Manager route pattern and a Cisco Expressway transform.

To set up simplified dialing, do the following:

Procedure

Step 1 Select a prefix beginning with a digit that is not frequently used in your dial plan. This can include * or #.

Step 2 On Unified Communications Manager, create a route pattern starting with the prefix, followed by a dot (period) character, and nine X characters representing the meeting number digits.

For example, for a prefix of 7 use 7.XXXXXXXXX

Step 3 Configure the route pattern to direct the call to the Cisco Expressway.

Step 4 On the Cisco Expressway, create a transform that matches any dial string starting with 7 followed by 9 digits.

For example, if a prefix of 7 uses a regex pattern string of 7(\d{9})@.* for a suffix being sent, or 7(\d{9}) when no suffix is sent at all, this depends on the device used and its configuration. You may need a rule for both scenarios.

Step 5 Configure the transform to strip the prefix digit (7 in this example) and append the domain (@webex.com), so that the call is routed to the appropriate Webex site.

For example, with the regex pattern above, use a replace string of \1@webex.com.

In this example, when a user dials 7123456789, the call is ultimately routed as 123456789@webex.com. The substitution happens both for devices that are registered to Unified Communications Manager and for remote devices that are registered to a Cisco VCS Expressway.

This simplification only applies to devices within your enterprise, joining meetings hosted by your own enterprise. Users who dial meetings hosted by other enterprises and external video participants must dial the full video dial string, including the domain.

Configure Site Administration Settings

You have access to Cisco Webex Site Administration through your Webex Account Team using a unique Webex Site Administration URL and password. As a site administrator, you must log in to integrate and provision your account during first-time setup. After you have completed the first-time setup, you can manage your account and access Webex user and administration guides for the services and features that have been configured on your site.

For more information on configuring your site administration settings, see Configure Cisco Webex Meetings.

Configure Microsoft Skype for Business (or Lync) Federation

Use this procedure to enable Skype for Business users to join your video meetings. No Cisco infrastructure equipment (e.g. Cisco Expressway, Cisco VCS or Unified Communications Manager) is required. The Skype for Business servers communicate directly with the Webex cloud.

Procedure

Step 1 Make sure that you have a Skype for Business Edge that is deployed according to Microsoft recommendations in your environment. See the library on Microsoft TechNet for your version of Skype for Business Server.

Step 2 Ensure that you have a public Certificate Authority (CA)-signed certificate deployed on your Skype for Business Edge. (This should already be in place if you have a functioning Skype for Business Edge with Federation enabled.)

Step 3 Configure federation in one of the following two ways:

- Follow the SIP federation guideline from Microsoft: https://technet.microsoft.com/en-us/library/jj618369(v=ocs.15).aspx. DNS SRV record for _sipfederationtls._tcp is required.
- Explicitly allow the domain webex.com in your Skype for Business server's list of trusted federation partners.

Step 4 Verify that your firewall is configured to permit the following TCP and UDP ports between your Skype for Business Edge and the Webex network.

Protocol	Port	Note
SIP signaling between Skype for Business Edge and Webex	TCP port 5061	Should already be permitted if you have a functioning Skype for Business Edge.
RTP media between Skype for Business Edge and Webex	UDP and TCP ports 56000 to 57000	Should already be permitted within the range 50000 to 59999 if you have a functioning Skype for Business Edge.

For more information on federation, see Microsoft’s online documents:

- Lync 2013: http://technet.microsoft.com/en-us/library/gg425908.aspx
- Office 365: Allow users to contact external Skype for Business users

Deploy with CA-Signed Certificates

Before you begin

Make sure you submit your certificate signing request to a public certificate authority that issues a certificate that Webex supports.

Webex supports certificates that are issued by specific Root Certificate Authorities. Certificate providers may have multiple Root Certificate Authorities and not all may be supported by Webex. Your certificate must be issued by one of the following Root Certificate Authorities (or one of their Intermediate Certificate Authorities) or the call from your Cisco Expressway-E or Cisco VCS Expressway will not be accepted by Webex:

- entrust_ev_ca
- digicert_global_root_ca
- verisign_class_2_public_primary_ca_-_g3
- godaddy_class_2_ca_root_certificate
- Go Daddy Root Certification Authority - G2
- verisign_class_3_public_primary_ca_-_g5

- verisign_class_3_public_primary_ca_-_g3
- dst_root_ca_x3
- verisign_class_3_public_primary_ca_-_g2
- equifax_secure_ca
- entrust_2048_ca

Note To use a certificate generated by entrust_2048_ca with Cisco VCS Expressway X7.2 (or a later version upgraded from X7.2), you must replace the Entrust Root CA certificate in the trusted CA list on the Cisco VCS Expressway with the newest version available from Entrust. You can download the newer entrust_2048_ca.cer file from the Root Certificates list on the Entrust web site (https://www.entrust.net/downloads/root_index.cfm).

- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- GlobalSign Root R1

Note Contact GlobalSign to rekey the certificate to R1 if they assign you any other value.

- thawte_primary_root_ca
- geotrust_primary_ca
- addtrust_external_ca_root

This list may change over time. For the most current information, contact Webex or review the information at the following link: https://collaborationhelp.cisco.com/article/WBX83490.

Procedure

	Command or Action	Purpose
Step 1	Generate Certificate Signing Request , on page 27	Use the Cisco Expressway-E (or Cisco VCS Expressway) to generate a Certificate Signing Request (CSR).
Step 2	Install the Signed SSL Server Certificate , on page 27	Load the SSL certificate on the Cisco Expressway-E (or Cisco VCS Expressway)
Step 3	Configure the Trusted CA List on the Cisco Expressway-E, on page 27	Ensure that the trusted CA list contains the correct certificates.

Generate Certificate Signing Request

For secure calling, use the Cisco Expressway-E (or Cisco VCS Expressway) to generate a Certificate Signing Request (CSR).

This procedure provides high-level steps. For detailed instructions, see the "Generating a certificate signing request" section of the applicable guide:

- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco VCS Certificate Creation and Use Deployment Guide

Procedure

Step 1 Generate a Certificate Signing Request (CSR).

Step 2 Download the CSR and submit it to your chosen root certificate authority (CA).

Most certificate authorities require the CSR to be provided in a PKCS#10 request format.

Step 3 Make sure that in response, your CA provides you with an SSL server certificate that includes both Server and Client Auth keys.

Install the Signed SSL Server Certificate

This procedure provides high-level information. For detailed instructions, see the see the section whose title begins with "Loading certificates and keys" in the applicable guide:

- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco VCS Certificate Creation and Use Deployment Guide

Procedure

After you receive the SSL server certificate from your public CA, load it on the Cisco Expressway-E (or Cisco VCS Expressway).

Configure the Trusted CA List on the Cisco Expressway-E

Two types of certificates must be present in the trusted CA list on your Cisco Expressway-E (or Cisco VCS Expressway) to complete the secure calling configuration:

- The root certificate (and intermediate certificate, if applicable) of the public CA that you used to sign your SSL server certificate.
- The certificates of the public CAs used by the Webex cloud. To obtain these certificates, copy and paste the contents of each of the following links into a separate text file with a .PEM extension:
  - QuoVadis Root CA 2

  For detailed instructions on configuring the trusted CA list, see the applicable guide:

- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco VCS Certificate Creation and Use Deployment Guide

To determine whether the trusted CA list already contains a CA certificate, do the following:

Procedure

Step 1 In Cisco Expressway-E or Cisco VCS Expressway:

- X8.1 and later, go to **Maintenance** > **Security certificates** > **Trusted CA certificate**.
- X7.2.3, go to **Maintenance** > **Certificate management** > **Trusted CA certificate**.

Step 2 Click **Show CA certificate**.

A new window displays the current Trusted CA list.

Step 3 Search for the name of the CA that issued the certificate, for example, QuoVadis Root CA2.

Verify the Service

Procedure

Step 1 Create a test host account and enable it for video device-enabled meetings. If you are using TSP audio, configure the host account with the teleconferencing access parameters for the TSP.

Step 2 Sign in to your Webex site as the test host, download Cisco Webex Productivity Tools, and set up your Webex Personal Room and host PIN, if applicable.

Step 3 Schedule a Webex meeting by using Webex Productivity Tools and verify the following:

- The meeting appears on the calendar.
- The test host receives the meeting confirmation email from Webex.

Step 4 Dial into your Webex Personal Room or scheduled Webex meeting and verify the following:

- There is two-way video between the Cisco Webex Meetings application and TelePresence, Jabber, Lync, or other video devices.
- Devices that support presentation sharing can do so.

CHAPTER 4

Video Meetings

- Using Both Cisco Collaboration Meeting Rooms Hybrid and Video Device-Enabled Cisco Webex Meetings Offerings Together, on page 29
- About TSP Audio, on page 29

Using Both Cisco Collaboration Meeting Rooms Hybrid and Video Device-Enabled Cisco Webex Meetings Offerings Together

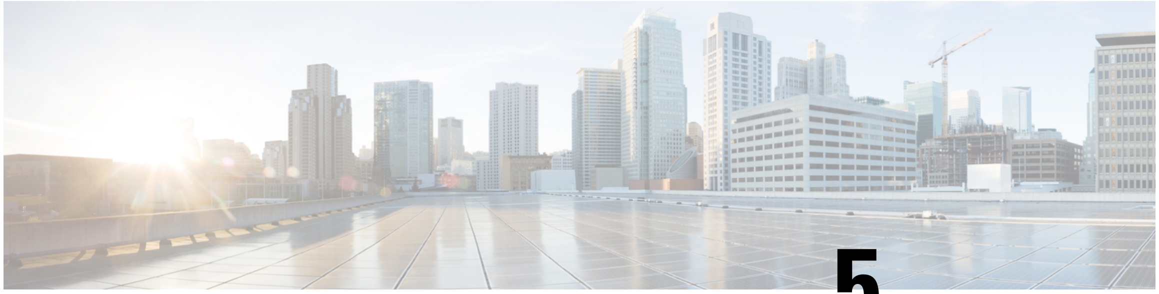
Hosts who have both video device-enabled meetings and CMR Hybrid can only use Webex Productivity Tools to manage video meetings.

Hosts who need to manage meetings using on-premises resources must use an alternate method, such as the Cisco Smart Scheduler or the Cisco Webex Scheduling Mailbox.

About TSP Audio

When you use video device-enabled meetings along with teleconferencing service provider (TSP) integrated audio, Webex establishes a PSTN call to the TSP audio service and uses a "script" of DTMF entries to join the audio conference. The phone number that is dialed, and the parameters necessary for this DTMF script, are obtained from the TSP Audio Account within the Webex host's account. These parameters are located under **My Webex** > **My Audio**.

Webex works with each TSP partner to determine the dial script to use (only Webex can view or modify the dial script).



CHAPTER 5

Configure One Button to Push

- One Button to Push, on page 31
- Configure Cisco TelePresence Management Suite Extension for Microsoft Exchange, on page 31
- Adding Cisco TMS Managed Endpoints to Exchange, on page 35

One Button to Push

One Button to Push (OBTP) allows meeting participants to join a video meeting directly by selecting the **Join Meeting** button. To take advantage of this capability, the room with the video must be added as a room resource in the Outlook calendar invite.

Note The host must have joined the meeting before attendees can use OBTP. If the host has not yet joined, attendees may be asked to enter the host PIN, press #, or enter a numeric password to join the meeting.

To enable OBTP, you must do the following:

- Configure Cisco Webex Productivity Tools with TelePresence from your Webex site. For details, refer to: Configure Site Administration Settings, on page 24.
- Configure TelePresence Management Suite (TMS) and TelePresence Management Suite Extension (TMS XE)
- Add TMS-managed endpoints to Microsoft Exchange

For more information, see Webex Integration to Microsoft Outlook for Windows Overview or Webex Integration to Outlook for the Mac Overview.

Configure Cisco TelePresence Management Suite Extension for Microsoft Exchange

Prerequisites

- Cisco TMSXE software release 5.2 or later is required.

- Cisco TMS software release 15.2 or later is required.
- Endpoints that are available as mailboxes for booking in a CMR Hybrid meeting must be set to AutoAccept in Exchange.
- If a meeting organizer is scheduling a meeting in a different domain than the domain in which the TMSXE is hosted, The domain in which the TMSXE resides must be added to the list of sites in the ‘Local intranet' zone on the meeting organizer's computer, so that it trusts the TMSXE server. If the TMSXE is hosted in a domain that is outside of the domain of many or all users, this can be done most efficiently by your company's IT group for all users via a group policy or logon script. If this is not done, each time a user tries to schedule a meeting, they will be required to enter their TMSXE username and password.
- A signed certificate that is trusted in the organization is required for TMSXE. To do this, you must generate a certificate signing request (CSR) from IIS to provide to the certificate authority (CA). The certificate can be a self-signed certificate or come from a trusted internal certificate authority or public certificate authority.

Deployment Best Practices

Cisco recommends installing Cisco TMSXE on a standalone server.

Cisco TMSXE may be co-located with Cisco TMS in smaller deployments, with the following prerequisites:

- The server must have a minimum of 4 GB RAM.
- A maximum of 50 telepresence endpoints are available for booking in Cisco TMS and Cisco TMSXE.

For details on installation and configuration of TMSXE, refer to the *Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide* that applies to your TMS version. Deployment guides appear under **Install and Upgrade Guides**:

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/products-installation-guides-list.html

Configuring Cisco TMSXE for One Button to Push

To configure Cisco TMSXE for scheduling using One Button to Push, you must perform the following:

- Install the CiscoTMS Booking Service

Installing the Booking Service

For details, refer to *Installing and configuring Cisco TMS Booking Service* in the *Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide* that applies to your TMS version. Deployment guides appear under **Install and Upgrade Guides**:

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/products-installation-guides-list.html

Configuring IIS for HTTPS

Booking Service requires HTTPS to be configured for DefaultSite in IIS.

If IIS is not present on the server before installation of Cisco TMSXE, it is automatically installed with Booking Service. HTTPS must then be configured after installation to allow Booking Service to operate.

For more information, refer to the Microsoft Support article: How To Set Up an HTTPS Service in IIS.

Note In the IIS configuration that is detailed in the link above, you must make the following setting for users to schedule meetings with the Webex and TelePresence Integration to Outlook plug-in for Microsoft Outlook: In the "SSL Settings" configuration for "Client certificates", you must select "Ignore". If you do not, users will receive a "hit a glitch" message when scheduling meetings using the Webex and TelePresence Integration to Outlook Plug-In for Microsoft Outlook.

Configuring the Server Certificate

On the windows server on which TMSXE is running, you must load a server certificate within IIS.

The process involves generating a certificate signing request (CSR), which is sent to a certificate authority (CA), and then installing the signed certificate you receive from the CA.

Generating a CSR for IIS 7 (Windows Server 2008)

Procedure

Step 1 Open the Server Manager console **(Start > All Programs > Administrative Tools > Server Manager**).

Step 2 In the Role View, select IIS Manager (**Server Manager > Roles > Web Server > IIS Manager**).

Step 3 Double-click **Server Certificates**.

Step 4 In the Actions pane on the right, click **Create Certificate Request**.

Step 5 (Important) In the "Common Name:" field, enter the Fully Qualified Domain Name (FQDN) of the DNS name which users will type into the address bar in their browser to reach your website (site.cisco.com NOT site). If you have a different physical hostname than what users will type into their browsers to get to your site, make sure to put in the name users will use.

Step 6 In the **Organization** field, type your organization name.

Step 7 In the **Organizational Unit** field, type the name of your organization and click **Next**.

Step 8 In the **City/locality** field, type the city where the server resides and click **Next**.

Step 9 In the **State/province** field, type the state where the server resides.

Step 10 In the **Country/Region** field, select US (United States) and click **Next**.

Step 11 Leave the CSP at the default value.

Step 12 For the **Bit Length**, select 2048.

Step 13 Enter (or Browse to) a filename to save the certificate request (CSR), click **Finish**.

Step 14 Copy and paste the entire contents of the CSR file you just saved.
The default save location is C:\.

Step 15 Provide the CSR file to your CA and wait for them to send a signed certificate back to you.

Installing the Public Root Certificate in IIS 7 (Windows Server 2008)

Procedure

Step 1 Double-click the **Root CA** certificate file and click **Install Certificate**.

Step 2 Click **Next**, place the radio button in **Place all certificates in the following store** and then click **Browse**.

Step 3 Place a check in **Show Physical Stores**.

Step 4 Expand the **Trusted Root Certification Authorities** folder, select the **Local Computer** folder, and click **OK**.

Step 5 Click **Next** and then **Finish**. You will receive the message: "The import was successful".

Installing the Intermediate CA Certificate (If Applicable)

Procedure

Step 1 Double-click the **Intermediate CA** certificate file and click **Install Certificate**.

Step 2 Click **Next**, place the radio button in **Place all certificates in the following store** and then click **Browse**.

Step 3 Place a check in **Show Physical Stores**.
Expand the **Intermediate Certification Authorities** folder, select the **Local Computer** folder, and click **OK**.

Step 4 Click **Next** and then **Finish**. You will receive the message: "The import was successful".

Installing the SSL Server Certificate

Procedure

Step 1 In the IIS Manager console, go to the **Server Certificates** action pane, and click **Complete Certificate Request**. The Complete Certificate Request Wizard appears.

Step 2 Browse to the location where you saved your SSL server certificate, select it, then click **Open**.

Step 3 Enter a friendly name for your certificate (use the certificate's hostname if you're unsure). Then click **OK**.
At this point SSL is available for TMSXE. You will still need to configure the TMSXE or individual directories to use SSL.Select your IIS Site.

Step 4 In the action pane on the right, under Edit Site, click **Bindings**.

Step 5 Click the **Add** button.

Step 6 In the Type menu, select **https**.

Step 7 In the SSL certificate menu, select your SSL certificate.

Step 8 Click **OK**.

Configuring the Location Displayed for TelePresence Rooms in Outlook

When selecting telepresence rooms while scheduling a video meeting in Outlook, the location of the room is displayed in the both the Select Attendees and Resources Address Book window, which is a standard part of Outlook, and the Select Telepresence Rooms window, which is displayed when using OBTP.

Procedure

Step 1 To display the Select Attendees and Resources Address Book window, click the **To...** button in the Meeting window.

Step 2 To display the Add Telepresence Rooms window, click the Add Telepresence Rooms button the Meeting Options pane.

Location in the "Select Telepresence Rooms" window is read from Active Directory upon startup of TMSXE for the Active Directory accounts of the enabled mailboxes and is provided to OBTP. It is a simple text field, and not structured data. The location information is the same as what is displayed in the "Location" column in the Microsoft Exchange Address Book, shown in Configuring Cisco TMSXE for One Button to Push.

The structure and hierarchy displayed in the drop-down menu in the Exchange Address Book is manually created by the Exchange administrator. This can be done by creating nodes, giving them a name and a search filter. A common use (besides geographical) is to structure the list using departments, groups or business units. For more information, refer to the documentation for Microsoft Exchange.

Adding Cisco TMS Managed Endpoints to Exchange

For details, refer to *Creating Mailboxes for Cisco TMS Endpoints in Exchange* in the *Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide* that applies to your TMS version. Deployment guides appear under **Install and Upgrade Guides**:

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/products-installation-guides-list.html

CHAPTER 6

Troubleshooting

- Troubleshooting Problems with TSP Audio, on page 37
- Packet Loss on MPLS or Site-to-Site VPN Networks, on page 37
- Version Compatibility, on page 38

Troubleshooting Problems with TSP Audio

Table 8: Problems with TSP Audio

Problem or Message	Possible Causes	Recommended Action
TelePresence participants cannot hear Webex participant audio.	The TSP Audio Account that is used by the Webex host account is not valid.	Verify the validity of the Audio Account by starting a Webex meeting (not a video meeting) using the same host account. Verify that telephony works by using the callback feature. If the callback fails, log into the Webex site as the same host used to schedule the meeting and edit or verify the validity of the default TSP Audio Account within the host account (My Webex > My Audio > Edit). You may need to contact your TSP service provider in order to get a valid TSP Audio Account.
	The PSTN/DTMF dial script is not successfully navigating the IVR of the TSP audio conference service.	Contact technical support. Be prepared to provide the details of the TSP Audio Account of the Webex host account being used for the meeting.

Packet Loss on MPLS or Site-to-Site VPN Networks

If you experience packet loss on MPLS or site-to-site VPN networks, make sure not to set MTU and DF-bit within the VCS/Expressway.

Version Compatibility

For all the information on video compatibility and support, see Webex Video Compatibility and Support.