Cisco Collaboration Meeting Rooms (CMR) Hybrid

Configuration Guide

TMS 14.4
WebEx Meeting Center WBS 29

OL-21352-02

Updated: July 2016

Contents

Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account 149

Scheduling CMR Hybrid Meetings 161

Troubleshooting 169

Preface

First Published: June 23, 2014

This preface describes the purpose, audience, organization, and conventions of the *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* and provides information about new features and how to obtain related documentation.

CMR Hybrid was formerly called WebEx Enabled TelePresence.

This preface contains the following topics:

General Description

This document describes how to configure Cisco TelePresence applications for Cisco WebEx-to-Cisco Telepresence interoperability. The *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* guide describes how to manage and monitor scheduled meeting interoperability between Cisco TelePresence System (CTS), Cisco TelePresence Server or Cisco TelePresence MCU Series multipoint meetings, Cisco TelePresence Management Suite, Cisco Unified Communications Manager (Unified CM), Cisco TelePresence Video Communication Server (Cisco VCS) and the Cisco WebEx Meeting Center.

The *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* is directed to administrators who will be configuring the Cisco TelePresence Server, Cisco TelePresence MCU Series, Cisco TelePresence Management Suite, TelePresence endpoints, Cisco TelePresence Video Communication Server or Cisco Expressway Series, and/or the Cisco Unified Communications Manager to use Cisco WebEx features in Cisco TelePresence meetings.

Cisco WebEx Features and Important Notes

This section contains the following feature information:

- Supported Features [p.8]
- Feature Limitations [p.9]

Supported Features

CMR Hybrid provides the following key features:

- Two-way video sharing with up to 720p screen resolution between the WebEx application and telepresence devices
- Integrated audio and presentation sharing — including application and desktop content sharing capability for all users in a meeting
- Network-based recording of meetings including content share, chat and polling
- Integrated meeting scheduling using Cisco TelePresence Management Suite (Cisco TMS), which allows you to easily schedule CMR Hybrid meetings
- Secure call control and connectivity enabled by media encryption provided by Cisco Expressway-E or Cisco VCS Expressway
- Unified CM-centric and VCS-centric call control deployment options
- Interoperability with third-party telepresence devices

Table 1: CMR Hybrid Features

Supported Feature	Description
Audio	TelePresence participants have two-way audio with the Cisco WebEx meeting participants using G.711 and G.722. **Note:** No presentation audio is sent from the Cisco WebEx side.
Host	The MCU/TS dials in at the meeting start time automatically to connect all TelePresence participants. The MCU/TS becomes the host if the meeting organizer has not joined on WebEx yet. If the meeting organizer joins the meeting on WebEx before the scheduled start time, they become the host.

Table 1: CMR Hybrid Features (continued)

Supported Feature	Description
Scheduling	Use Cisco TMS, the WebEx and TelePresence Integration to Outlook, Smart Scheduler, or WebEx Scheduling Mailbox to schedule a Cisco TelePresence meeting with WebEx. Start your meeting either using One-Button-to-Push (OBTP) from scheduled Cisco TelePresence endpoints or using the Automatic Connect feature of Cisco TMS to connect all scheduled endpoints at the start time of your meeting. You can start the WebEx portion of a Cisco Collaboration Meeting Rooms (CMR) Hybrid meeting earlier than the scheduled time if you are the WebEx host. WebEx participants who try to join the WebEx meeting before the host, receive a message that the meeting has not started and they must wait to join until the scheduled start time or until after the WebEx host joins. **Note:** Only scheduled meetings are supported for Cisco Collaboration Meeting Rooms (CMR) Hybrid Interoperability; non-scheduled TelePresence participants who want to join a Cisco Collaboration Meeting Rooms (CMR) Hybrid meeting, must manually dial into the conference (MCU/TelePresence Server) bridge. The meeting organizer reserves ports for video dial-in participants when scheduling the meeting. See Cisco TelePresence Management Suite Administrator Guide for meeting scheduling information.
Sharing	Cisco TelePresence users can share a presentation by connecting the video display cable of the TelePresence endpoint to their computer. Supported video display interfaces include VGA, DVI, HDMI, DisplayPort and Mini DisplayPort. Cisco WebEx Meeting Center clients can share the desktop or a selected application. Endpoints view and share Cisco WebEx presentation at 1024 x 768 (XGA) resolution. The resolution that endpoints are capable of sending may vary depending on the endpoint model, but the TS/MCU transcodes the presentation and sends it to the WebEx cloud at 1024 x 768 resolution.
Two-way Video	Video from Cisco TelePresence endpoints is sent to Cisco WebEx participants and video from Cisco WebEx participants is sent to Cisco TelePresence endpoints. Live video can be sent at minimum in Common Intermediate Format (CIF) format at 30 frames per second, at approximately 300-450 kbps up to a maximum of 720p. Presentations from the Cisco WebEx client are displayed on each TelePresence endpoint. **Note:** All CMR Hybrid meetings require the use of a Cisco TelePresence Server or MCU.

Feature Limitations

For a complete list of limitations and known issues for CMR Hybrid, refer to the CMR Hybrid release notes.

Prerequisites

Table 2: Cisco WebEx with the Cisco TelePresence System

Requirement	Description
Cisco TelePresence Management Suite (Cisco TMS)	Cisco TMS is required for scheduling CMR Hybrid meetings. Release 14.4 or later is required.
Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE)	Cisco TMSXE is required for scheduling CMR Hybrid meetings through Microsoft Outlook using either the WebEx Productivity Tools Plug-in or WebEx Scheduling Mailbox Scheduling. Release 3.1 or later is required. 4.0 or later is recommended (supports Microsoft Exchange 2013).
Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE)	Cisco TMSPE is required for scheduling Cisco Collaboration Meeting Rooms (CMR) Hybrid meetings using Smart Scheduler. Release 1.1 or later is required. 1.2 is recommended. Use of Smart Scheduler does not require the TMS provisioning option key.
Cisco TelePresence Video Communication Server (Cisco VCS)	Cisco VCS Control and Cisco VCS Expressway are required as the call control solution. Release X7.2.3 or later is required. (The procedures in this document will work with release X7.2.2, however, we recommend that you upgrade to X7.2.3 to avoid the OpenSSL Heartbleed vulnerability.) **Note:** Customers using Static NAT on VCS Expressway X7.2.3 are highly recommended to not upgrade to X8.1 or X8.2 due to a defect that will cause the media part of a call to fail. Customers using Static NAT on their VCS Expressways running X7.2.2 are recommended to upgrade to release X7.2.3. If you are already using Static NAT with Expressway-E or VCS Expressway X8.1 or X8.2, refer to the recommended workarounds in Configuring Cisco Expressway and TelePresence Video Communication Server [p.61].
Cisco Expressway	Cisco Expressway-C and Cisco Expressway-E X8.1 or later are highly recommended for Unified CM-centric deployments because of the lower-cost licensing model and simplified deployment. **Note**: A Unified CM license is required to purchase Cisco Expressway.
Cisco Unified Communications Manager (Unified CM)	Unified CM is required for Unified CM-centric deployments and can also be used with VCS-centric deployments if endpoints are registered to Unified CM. Release 8.6.2 or later is required. Release 9.1.2 or 10.5 or later is required for Unified CM-centric deployments. Version 10.5.1 is recommended.
Cisco TelePresence Server	TelePresence Server can be used as a conference bridge for Cisco Collaboration Meeting Rooms (CMR) Hybrid meetings. Release 3.0 or later is required. Release 3.1 or later is required for support of TSP audio. Release 4.0 or later no longer requires the Third Party Interop feature key.

Table 2: Cisco WebEx with the Cisco TelePresence System (continued)

Requirement	Description
Cisco TelePresence MCU Series	Cisco TelePresence MCU Series can be used as a conference bridge for Cisco Collaboration Meeting Rooms (CMR) Hybrid meetings. Release 4.4 or later is required. Release 4.5 is required for Unified CM-centric deployments.
Provisioning—CMR Hybrid	1. The Cisco WebEx Meeting Center site must be running release WBS28.10 or higher with the latest service pack. 2. The Cisco WebEx site must be configured to support Cisco TelePresence Integration. See Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.149] for more information.
Supported Endpoints	Any endpoint supported by TelePresence Server or MCU can join a CMR Hybrid meeting. In order to present to WebEx participants, the endpoint must support the BFCP protocol.
Account Validation—Meeting scheduler's Cisco WebEx account.	Each user who is scheduling Cisco Collaboration Meeting Rooms (CMR) Hybrid meetings in Cisco TMS, must have a host account on the WebEx site. 1. The WebEx account username and password must be added into to each meeting scheduler's user profile in Cisco TMS, along with the WebEx site they will use for scheduling. 2. Cisco TMS validates authorized Cisco WebEx account holders. **Note:** WebEx password is not required if Single-Sign-On (SSO) is configured in TMS. See Configuring Cisco TelePresence Management Suite [p.97] for more information.
Bandwidth and CPU power—Recommendation for good video quality and integrating the Cisco TelePresence network with Cisco WebEx.	Network bandwidth should be at least 2-4 Mbps upstream between the MCU/TelePresence Server and Cisco WebEx. For example, if you are anticipating 5 simultaneous Cisco WebEx calls, you will need to have five 2-4 Mbps bandwidth instances. Suggested CPU power (depends on running applications) is dual core CPU, 2.5 GHz memory running at least 2G.
Cisco WebEx Meeting Center Requirements—Expected resource allocation per meeting.	For detailed requirements, refer to the CMR Hybrid release notes. Guidelines: ■ Bandwidth must be at least 1.3 Mbps per WebEx Meeting Center client for the best possible experience. ■ Where WebEx clients connect via TCP they will be less tolerant of network impairments and more likely to request a downspeed from WebEx vs UDP. Open UDP ports 9000/9001 to WebEx Meeting Center clients.

Table 2: Cisco WebEx with the Cisco TelePresence System (continued)

Requirement	Description
Network Access	To ensure best results with CMR Hybrid, Cisco recommends customers to allow connectivity to all of the following IP and port ranges:

IP Ranges

US/Canada

- 64.68.96.0/19 (CIDR) or 64.68.96.0 - 64.68.127.255 (net range)
- 66.114.160.0/20 (CIDR) or 66.114.160.0 - 66.114.175.255 (net range)
- 66.163.32.0/20 (CIDR) or 66.163.32.0 - 66.163.47.255 (net range)
- 208.8.81.0/24 (CIDR) or 208.8.81.0 - 208.8.81.255 (net range)
- 209.197.192.0/19 (CIDR) or 209.197.192.0 - 209.197.223.255 (net range)
- 173.243.0.0/20 (CIDR) or 173.243.0.0 - 173.243.15.255 (net range)

APJC

- 210.4.207.48/28
- 210.4.206.48/28
- 210.4.207.0/27
- 210.4.206.0/27
- 114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range)

EMEA

- 62.109.192.0/18

Ports Used by WebEx Client for Inbound and Outbound Communication (Windows and Mac)

Protocol	Port Number	Access Type
TCP	80	Client Access
TCP	443	Client Access - Secure Traffic (SSL Sites)
TCP/UDP	1270	Client Access (Non SSL Sites)
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	5101	Multi Media Processor (MMP)
TCP	8554	Audio Streaming Client Access
UDP	7500	Audio Streaming
UDP	7501	Audio Streaming
UDP	9000	VoIP/Video
UDP	9001	VoIP/Video

Table 2: Cisco WebEx with the Cisco TelePresence System (continued)

<table>
<tr><th>Requirement</th><th>Description</th></tr>
<tr><td></td><td>Ports Used by Expressway-Edge or VCS-Expressway for Outbound Calls from TelePresence Endpoints
<table><tr><th>Protocol</th><th>Port Number</th><th>Access Type</th></tr><tr><td>TCP</td><td>5060 - 5065</td><td>Call Signaling (Primary and Backup)</td></tr><tr><td>UDP</td><td>36000 - 59999</td><td>Call Media (Primary and Backup)</td></tr></table>
<b>IMPORTANT</b>: Firewalls, ports and protocols that do deep packet inspection should not be used. Specifically, the stateful packet inspection used in Check Point Software Technologies, Inc. firewalls is incompatible with Cisco VCS Expressway and Expressway-E.
As a result, it is highly recommended to disable SIP and H.323 application layer gateways on routers/firewalls carrying network traffic to or from a VCS Expressway or Expressway-E, because, when these are enabled they can negatively affect the built-in firewall/NAT traversal functionality of the VCS</td></tr>
<tr><td>Network Requirements and Recommendations</td><td>To ensure best results with CMR Hybrid, customer should comply with the following network requirements and recommendations:
■ UDP connection from customer premises to WebEx with no more than 6-8% packet loss. Make sure UDP is selected in the WebEx Site Administration settings. For details, refer to Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.150]
■ Network connection from customer premises to WebEx over the public Internet must not exceed 1% packet loss. To achieve satisfactory video quality, packet loss should be below 0.05%.</td></tr>
</table>

Network Requirements for CMR Hybrid

Table 3: CMR Hybrid Network Requirements

Network Leg		Packet Loss	Latency [RT]	Jitter	Min. Bandwidth required for Video	Min. Bandwidth required for Sharing
Leg 1	MCU to WebEx	Good=<0.05% OK=<1%	Good =<150ms OK =<250ms	Cumulative jitter across all legs between hops with jitter buffers, i.e. MCU@Leg1<->Wx client@Leg3 (as measured by a WX client, e2e) MUST be less than ~40-50 ms.	2-4 Mbps per concurrent CMR Hybrid meeting	
Leg 2	TelePresence Endpoints to MCU	Varies by capability Good~=<1% OK~=<1-10%*	Good =<200ms OK =<300ms		1-4 Mbps per TelePresence Endpoint or Jabber Client	
Leg 3	WebEx clients to WebEx [UDP]	Good = <2% OK = <6-8%	Good =<300ms		512kbps video +768kbps presentation = ~1280kbps total	XGA =768kbps (share only) 720p =2Mbps 1080p=3Mbps*
Leg 3	WebEx clients to WebEx [TCP]	Good = <1% OK = <1-2%	Good =<200ms		512kbps video +768kbps presentation = ~1280kbps total	XGA =768kbps (share only) 720p =2Mbps 1080p=3Mbps*

Document Organization

Information about configuring and using the CMR Hybrid is provided in the following chapters:

Related Documents

Related Topic	Link to documentation overview on cisco.com
Cisco TelePresence Documentation	
Cisco TelePresence Management Suite	Cisco TelePresence Management Suite
Cisco TelePresence Video Communication Server (Cisco VCS)	Cisco TelePresence Video Communication Server
Cisco Unified Communications Manager (Unified CM)	Cisco Unified Communications Manager
Cisco TelePresence Server	Cisco TelePresence Server
Cisco TelePresence MCU Series	■ MCU 5300 Series ■ MCU 4501 Series ■ MCU 4500 Series ■ MCU 4200 Series ■ MCU MSE Series
Cisco WebEx Documentation	
Information about how to use Cisco WebEx meeting features.	■ Go to your Cisco WebEx site home page. ■ Log into your Cisco WebEx Meeting Center account and click on **Support > User Guides** in the left navigation pane.
Specifying Cisco TelePresence Integration options and managing your Cisco WebEx Site.	See Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.149].
Cisco Collaboration Meeting Rooms (CMR) Hybrid Documentation	
Information for meeting organizers on how to schedule CMR Hybrid meetings	http://www.cisco.com/en/US/products/ps11338/products_user_guide_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at the following URL:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Information About the CMR Hybrid Solution

First Published: June 23, 2014

This chapter provides an overview of the CMR Hybrid solution. It contains the following sections:

CMR Hybrid Experience

This section contains the following information about the Cisco Collaboration Meeting Rooms (CMR) Hybrid meeting experience:

- Scheduling the Meeting [p.19]
- Starting/Joining the Meeting [p.19]
- Cisco TelePresence Meeting Experience [p.19]
- Cisco WebEx Meeting Experience [p.20]

Scheduling the Meeting

The meeting organizer can schedule the meeting using the Cisco WebEx and TelePresence Integration to Outlook, Cisco Smart Scheduler, Cisco TelePresence Management Suite (Cisco TMS) or Cisco WebEx Scheduling Mailbox.

For more information about how to schedule a meeting using the different scheduling options, see Scheduling CMR Hybrid Meetings [p.161].

Starting/Joining the Meeting

The meeting starts the following way:

- At the scheduled start time of the meeting, the MCU/TelePresence Server calls into WebEx.
  - If the WebEx host has not joined the meeting, the MCU/TelePresence Server becomes the default WebEx host.
  - If the WebEx host joins before the scheduled start time of the meeting, he/she becomes the WebEx host.
- Telepresence participants join the meeting.
  - If meeting was scheduled using Auto Connect, Cisco TMS dials and connects each supported endpoint.
  - If meeting was scheduled using One-Button-to-Push (OBTP), participants using endpoints that support OBTP press the button on their endpoint to join the meeting.
  - Participants using endpoints that don't support either Auto Connect or OBTP, join the meeting by dialing the video dial-in number listed in the meeting invitation.
- WebEx participants join the meeting by using the link in the meeting invitation.

Cisco TelePresence Meeting Experience

Cisco TMS is used to configure and manage the Cisco WebEx bridging feature in Cisco TelePresence meetings. During the meeting, telepresence participants see live video of all other telepresence participants, and the video of the most recently active WebEx participant. WebEx participants see the video of all other WebEx participants, and the video of the most recently active telepresence participant.

The Cisco WebEx bridging feature integrates the Cisco WebEx conferencing server with multipoint meetings on the Cisco TelePresence MCU Series or Cisco TelePresence Server. Cisco Telepresence callers connect to meetings using One-Button-to-Push (OBTP) or Automatic Connect technology. The MCU/TelePresence Server connects at the meeting start time, automatically connects with the Cisco WebEx conference and joins the two meetings. Upon connecting with Cisco WebEx, the Cisco Telepresence presentation screen shows a Welcome page.

For presentation sharing, the telepresence user connects the video display cable to their computer and (if required) presses a button to start sharing their presentation to telepresence and WebEx participants. Video of the active telepresence speaker is streamed to the Cisco WebEx Web client. Video and presentation from WebEx is visible to telepresence participants.

Cisco WebEx Meeting Experience

Remote participants join the Cisco WebEx meeting by logging in to the Cisco WebEx Meeting Center Web and/or mobile applications*. Content shared by a Cisco TelePresence participant is displayed automatically in the Meeting Center application, and WebEx participants can share their desktop or application with Cisco TelePresence participants. By default, WebEx participants see the live video of the actively speaking Cisco TelePresence or WebEx participant.

WebEx participants also see an integrated list of all WebEx meeting participants. The WebEx annotation feature is supported. WebEx participants can annotate using the standard Meeting Center application annotations tools and both WebEx and TelePresence participants can see the annotations. The annotation tools are not available, however, for TelePresence participants.

When the first WebEx participant joins, "TelePresence systems" appears in the list of WebEx participants (Figure 1: Cisco WebEx Meeting—Default View [p.21]) and in the row of WebEx participants in Full Screen view (Figure 2: Cisco WebEx Meeting—Full Screen View [p.22]). This indicates that it is a Cisco CMR Hybrid meeting. Individual TelePresence users are not listed in the WebEx participants list. Instead, only "TelePresence systems" is listed and is displayed in the active speaker window when a TelePresence participant is the active speaker.

For WebEx participants to share their presentation with TelePresence participants, they must do the following:

1. Log into the Cisco WebEx Meeting Center application on their computers.
2. Grab the ball or be designated as presenter by the WebEx host.
3. Start application or desktop sharing.

* For a list of supported mobile clients, refer to the Cisco Collaboration Meeting Rooms (CMR) Hybrid release notes.

Recommended Screen Resolutions for Presentation Sharing

To utilize the full screen while presenting, Cisco recommends setting your computer to a 4:3 aspect ratio screen resolution. The following screen resolutions are recommended:

- 1024 x 768
- 1152 x 864
- 1280 x 1024
- 1600 x 1200

Passing the Ball

WebEx users share a presentation by taking the ball and then selecting the content to present. If the WebEx site does not allow WebEx participants to take the ball, the WebEx host must pass the ball to the WebEx participant. Alternately, an attendee can use the host key to become the new host. Then this new host can assign the presenter ball to him/herself to present. For more information about using Cisco WebEx meeting functions, log into your Cisco WebEx Meeting Center account and click **Support** in the left navigation pane.

Viewing the Meeting in WebEx

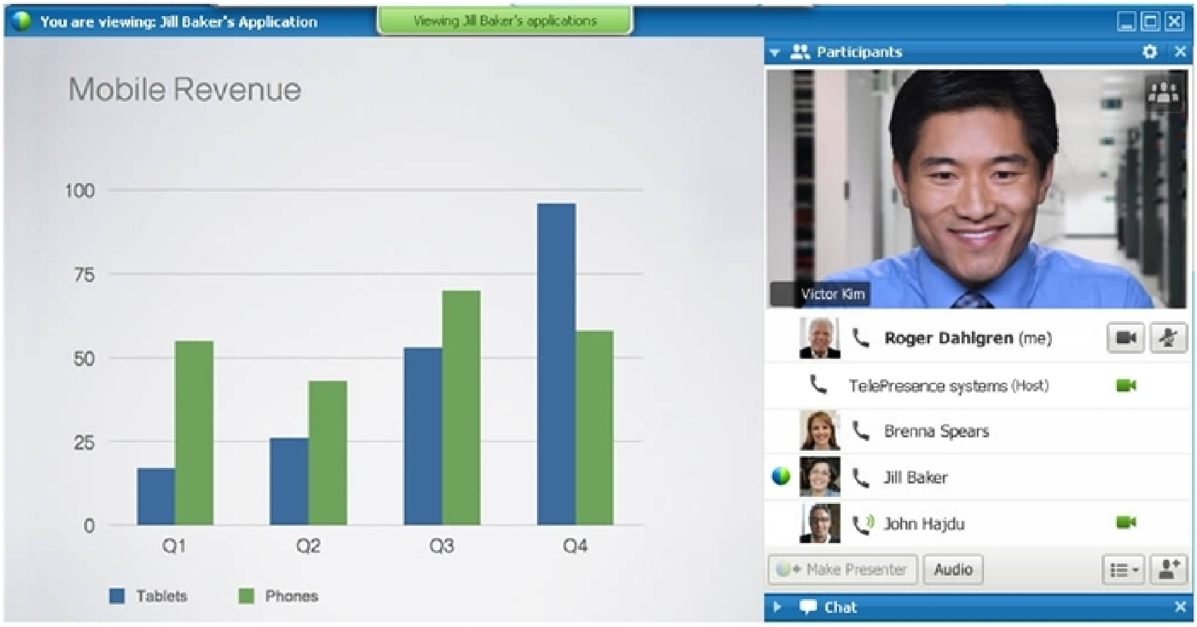
When attending the meeting using the WebEx Meeting Center web client (Windows or Mac), you have two basic ways to experience the meeting:

- Default View
- Full Screen view

Default View

When you log in to the meeting, the WebEx client displays the default view (see Figure 1: Cisco WebEx Meeting—Default View [p.21]). The default view displays a video window and participant list on the right and the presentation being shared on the left. The video window shows the current active speaker (either TelePresence or WebEx).

Figure 1: Cisco WebEx Meeting—Default View



Full Screen View

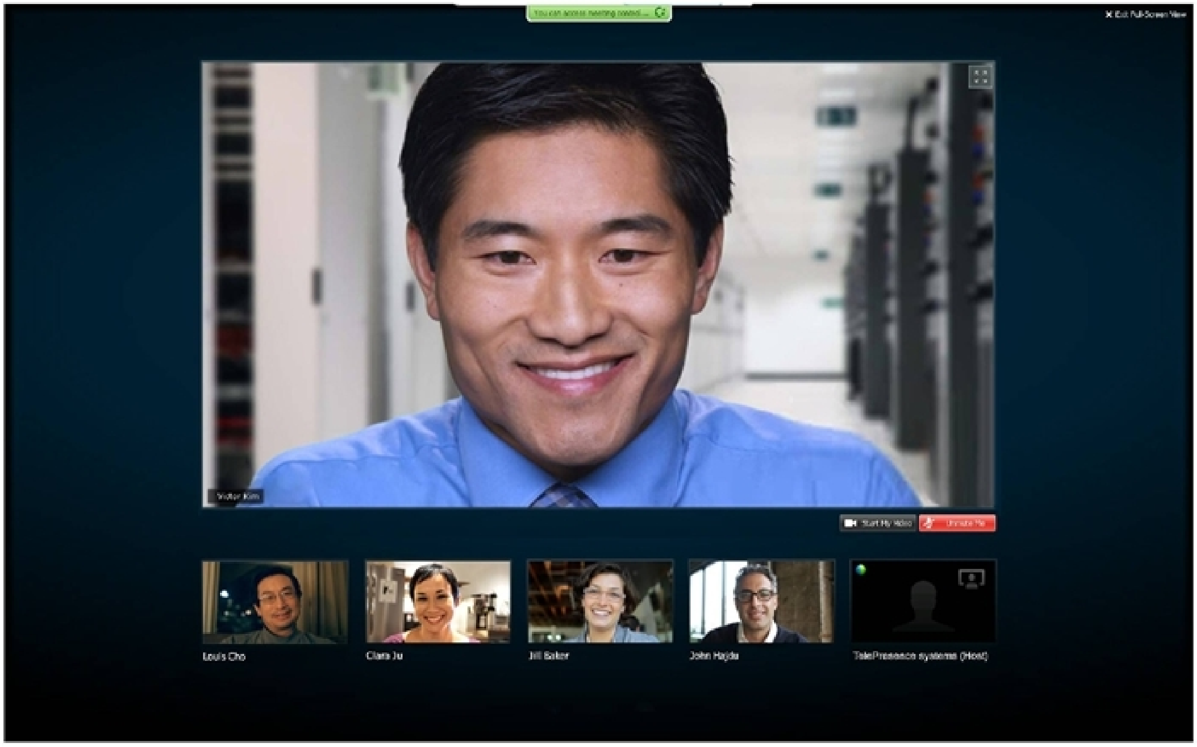
Full Screen view displays the active speaker in a large image at the top of the window and WebEx participants at the bottom of the window (see Figure 2: Cisco WebEx Meeting—Full Screen View [p.22]). When in Full Screen mode, the presentation is not visible.

WebEx participants can go into Full Screen mode to see all of the other WebEx participants. While in Full Screen mode, a participant sees all other WebEx participants plus the video of a TelePresence participant when the participant is the active speaker.

To go into Full Screen mode, click the Full Screen button in the video window in the default view.

Cisco TelePresence Server or MCU can be configured to display other TelePresence participants in the active speaker window. See CMR Hybrid Experience [p.19] for an example of ActivePresence enabled by default on the TelePresence Server. MCU sends a full screen layout.

Figure 2: Cisco WebEx Meeting—Full Screen View



Understanding How CMR Hybrid is Deployed

CMR Hybrid can be deployed in either of the following networks:

- Cisco Unified-CM-centric networks
- Cisco VCS-centric networks

The supported deployment models are described in the next section: Deployment Scenarios [p.24].

Note: Unified CM-centric deployments require Unified CM 9.1.2, 10.5 or later and (if used) MCU software release 4.5 or later.

Deployment Scenarios

Unified CM-centric Deployments

There are three possible network topologies for CMR Hybrid using a Unified CM-centric deployment model:

- SIP Video, Presentation, and Audio in a Unified CM-centric Deployment [p.24]
- SIP Video, Presentation, and PSTN Audio in a Unified CM-centric Deployment [p.25]:
  - Using a gateway registered to Unified CM
  - Using a gateway registered to Cisco Expressway-C

Note: In a Unified CM-centric deployment, Cisco Expressway-C and E are recommended by Cisco because of lower cost and complexity, but Cisco VCS Control and Expressway are also supported.

Cisco VCS-centric Deployments

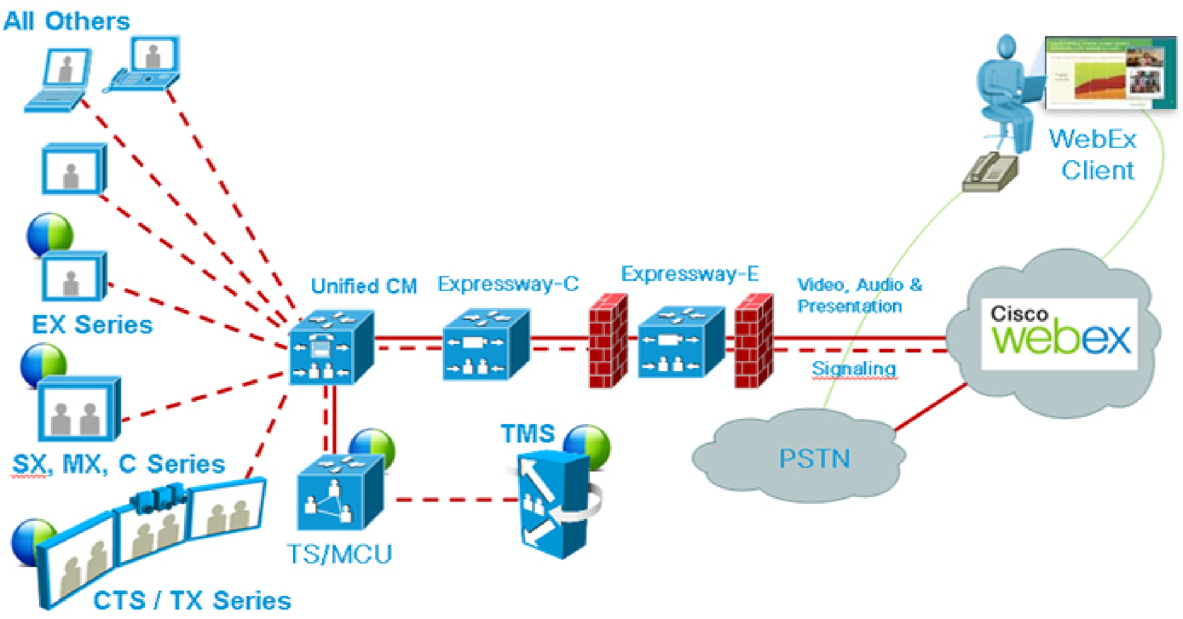
There are three possible network topologies for CMR Hybrid using a VCS-centric deployment model:

- SIP Video, Presentation, and Audio in a VCS-centric Deployment [p.27]
- SIP Video, Presentation, and PSTN Audio in a VCS-centric Deployment [p.27]:
  - Using a gateway registered to Unified CM
  - Using a gateway registered to Cisco VCS Control

SIP Video, Presentation, and Audio in a Unified CM-centric Deployment

WebEx is deployed using WebEx Audio. Main video, content, and audio to and from the WebEx cloud is negotiated between the Cisco Expressway-E on the customer site and the WebEx Cloud. All media (main video, content, and audio) flows over IP negotiated using SIP. Blue and green balls symbolize WebEx-enabled endpoints (ball displayed on endpoint display) (OBTP).

Figure 3: Network Topology - SIP Video, Audio and Presentation



SIP Video, Presentation, and PSTN Audio in a Unified CM-centric Deployment

WebEx is deployed using WebEx Audio using PSTN. Only main video and content is negotiated through the Cisco Expressway-E on the customer site and WebEx cloud (SIP/IP).

At the time of scheduling, Cisco TMS provides the MCU PSTN access information (Dial number, Conference ID, Attendee ID). The Cisco MCU calls out and sets up the audio-only call over PSTN to the WebEx cloud, passing the conference ID and attendee ID using DTMF.

This deployment can be set up either of the following ways:

- Using a PSTN gateway registered to Unified CM - See Figure 4: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified CM [p.26].
- Using a PSTN gateway registered to Cisco Expressway-C- See Figure 5: Network Topology - SIP Video and Presentation with PSTN Audio Using Cisco Expressway-C [p.26].

Note: Customers using a Codian ISDN Gateway must register it to Cisco VCS Controland therefore must use Cisco VCS.

Figure 4: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified CM

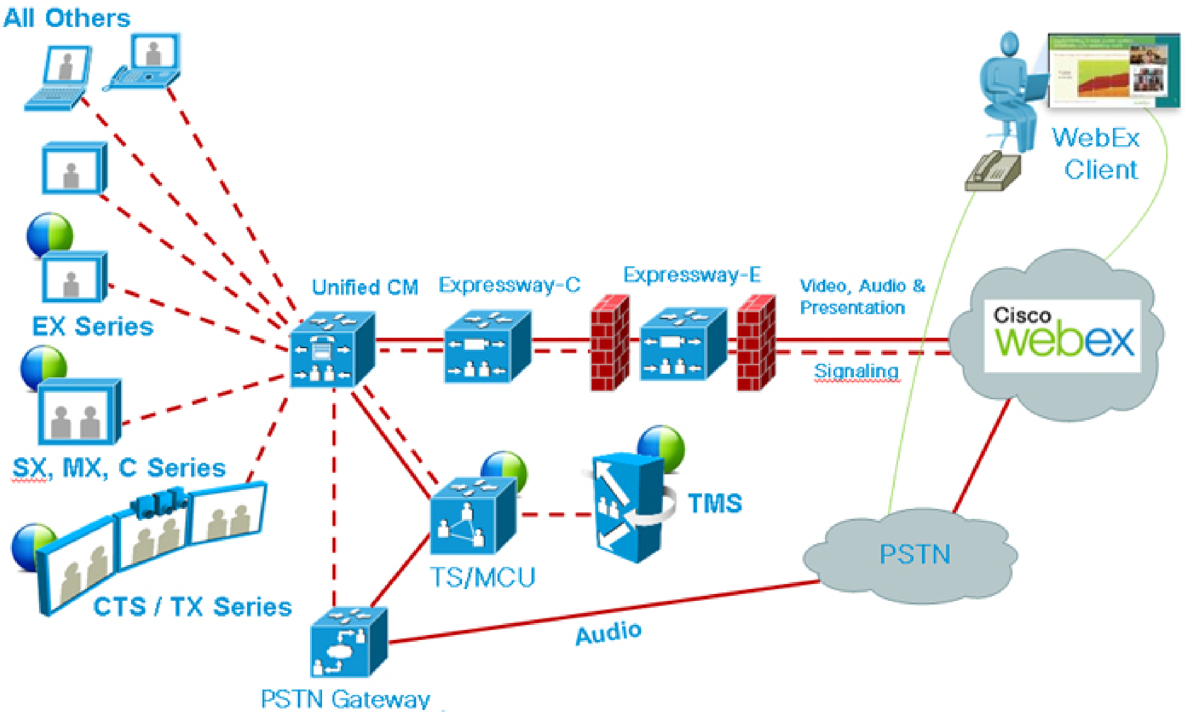
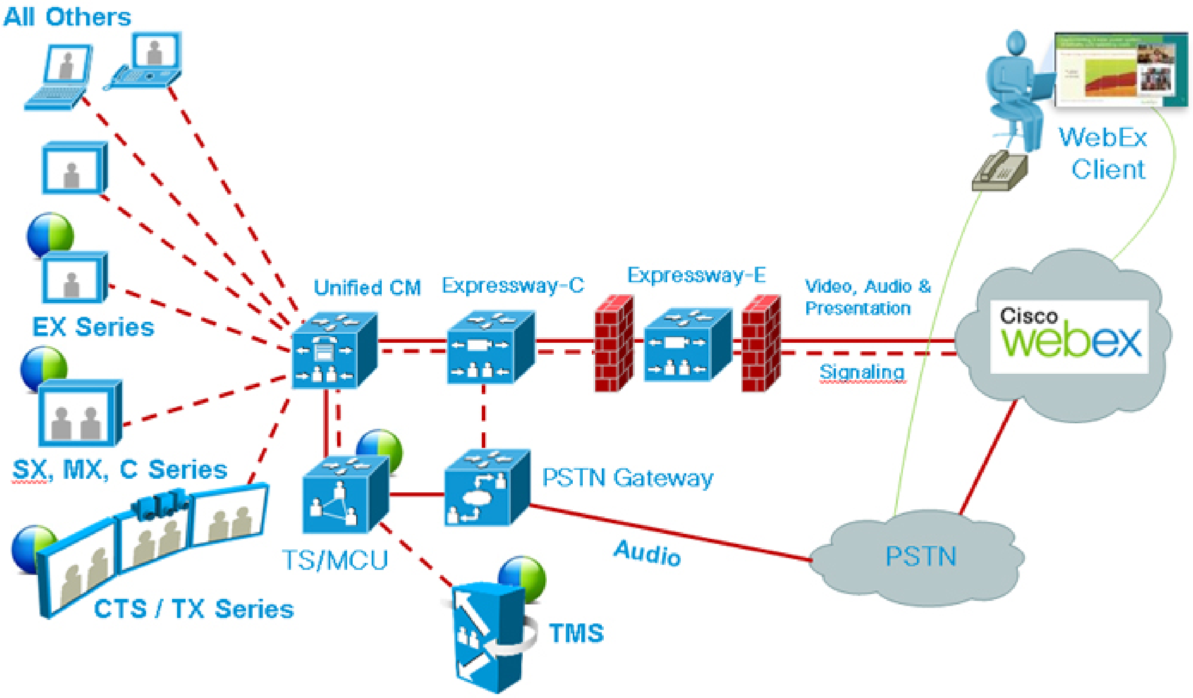


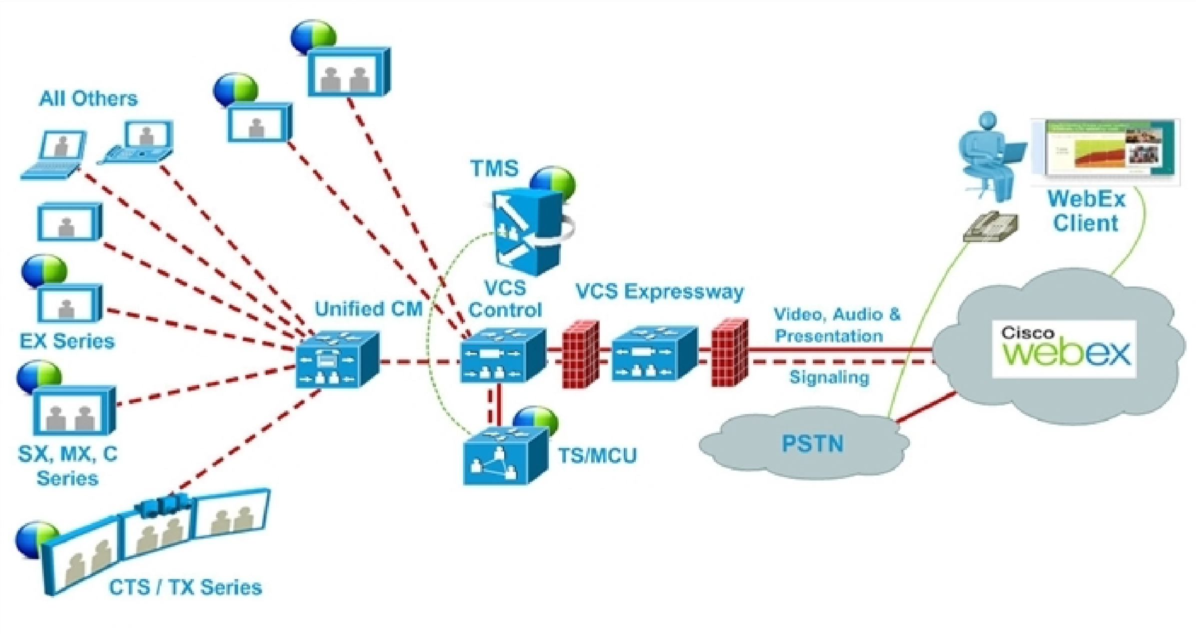
Figure 5: Network Topology - SIP Video and Presentation with PSTN Audio Using Cisco Expressway-C



SIP Video, Presentation, and Audio in a VCS-centric Deployment

WebEx is deployed using WebEx Audio. Main video, content, and audio to and from the WebEx cloud is negotiated between the Cisco VCS Expressway on the customer site and the WebEx Cloud. All media (main video, content, and audio) flows over IP negotiated using SIP. Blue and green balls symbolize WebEx-enabled endpoints (ball displayed on endpoint display) (OBTP).

Figure 6: Network Topology - SIP Video, Audio and Presentation



SIP Video, Presentation, and PSTN Audio in a VCS-centric Deployment

WebEx is deployed using WebEx Audio using PSTN. Only main video and content is negotiated through the Cisco VCS Expressway on the customer site and WebEx cloud (SIP/IP).

At the time of scheduling, Cisco TMS provides the MCU PSTN access information (Dial number, Conference ID, Attendee ID). The Cisco MCU calls out and sets up the audio-only call over PSTN to the WebEx cloud, passing the conference ID and attendee ID using DTMF.

This deployment can be set up either of the following ways:

- Using a PSTN gateway registered to Unified CM - See Figure 7: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified CM [p.28].
- Using a PSTN gateway registered to VCS - See Figure 7: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified CM [p.28].

Figure 7: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified CM

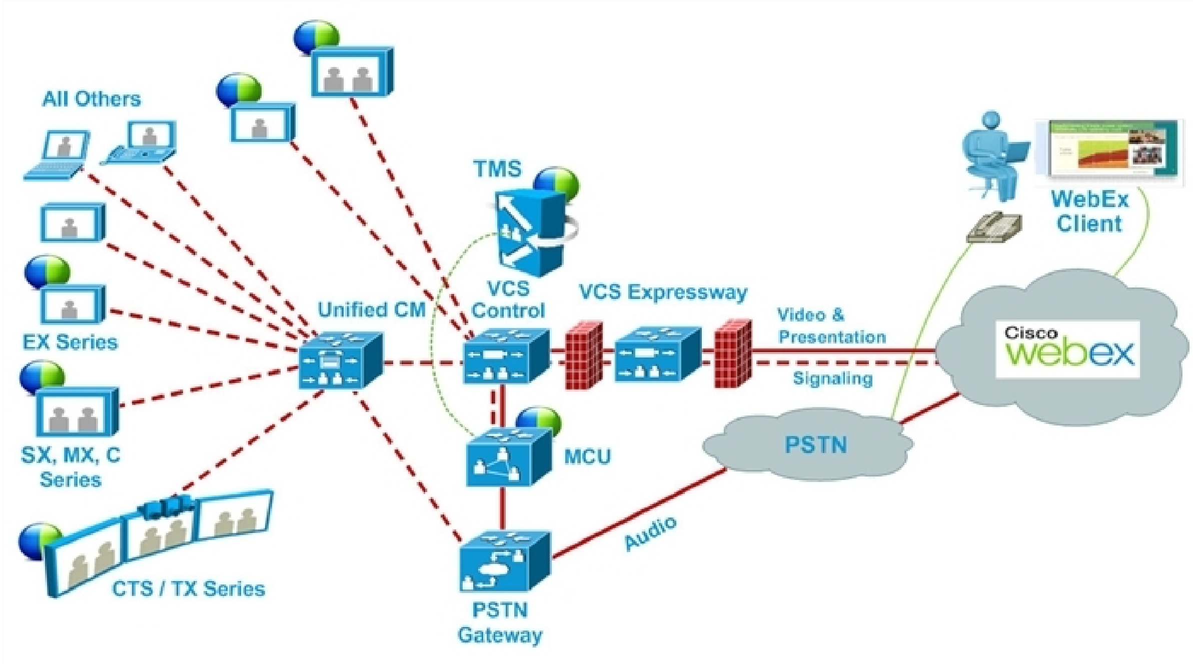
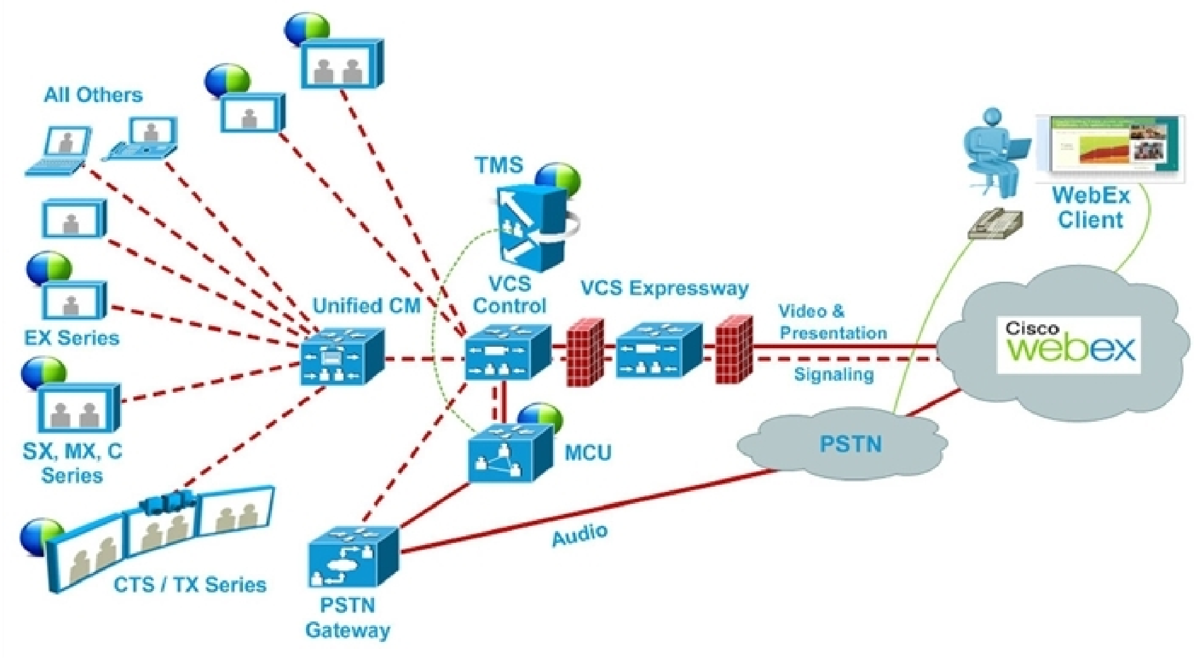


Figure 8: Network Topology - SIP Video and Presentation with PSTN Audio Using Cisco VCS Control



Cisco TMS Scheduling Role

Cisco TMS provides a control link to the Cisco WebEx site. This interface allows Cisco TMS to book a WebEx-enabled meeting on behalf of the WebEx Host, and to obtain Cisco WebEx meeting information that is distributed to meeting participants.Cisco TMS then pushes Cisco WebEx meeting details to the TelePresence Server/MCU.

TelePresence Server and MCU Roles

Cisco TelePresence Server/MCU will send/receive two-way main video with up to 720p30 between WebEx Meeting Center clients and TelePresence endpoints. The MCU/TS sends a single transcoded video stream to the WebEx Meeting Center client.

The MCU/TS will send a single mixed audio stream of the TelePresence meeting participants to the WebEx cloud. Likewise, the MCU/TS will receive a single mixed audio stream from all WebEx participants, including WebEx Meeting Center participants joined over PSTN or VoIP.

Support for two-way content share XGA (1024 x 768) resolution between telepresence endpoints and WebEx clients.

Each meeting creates its own SIP connection to avoid Transmission Control Protocol (TCP) congestion and potential TCP windowing issues.

MCU/Cisco TelePresence Server connects automatically at the meeting's scheduled start time.

Presentation Display Details for Multiple Presenters

For TelePresence participants to present, the presenter connects the video display cable to the endpoint and (if necessary) presses a presentation button on the endpoint. When multiple TelePresence participants are presenting at the same time, the endpoint that started presenting last is the one that is displayed. As cables are unplugged, the next presenter must start presenting again.

For WebEx participants to present, they grab the ball and then select the content to present. If a WebEx user cannot grab the ball, the host must pass it to them. Alternatively, they can use the host key to become the new host.

Note: The WebEx site can be provisioned so that any WebEx attendee can grab the ball to present without the host passing them the ball or using the host key.

Meeting Participants List

The TelePresence participant list, a roster of endpoint names currently connected to the Cisco TelePresence Server (if used), is displayed on the TelePresence endpoint display device. MCU and certain endpoint models do not support this feature.

The TelePresence participant list is not, however, displayed in the participant list available to WebEx users. WebEx users see only other WebEx participants and one participant called "TelePresence systems" that identifies all TelePresence participants in the meeting.

Ports and Protocols Used in CMR Hybrid

The following ports and protocols are used between different components of the CMR Hybrid solution.

Component Communication	Port and Protocol Used
Cisco TMS to WebEx cloud	Ephemeral port using TLS.443
WebEx and TelePresence Integration to Outlook to Cisco TMSXE	Ephemeral port using TLS.443
Cisco VCS Expressway to WebEx cloud	Set in accordance with the traversal subzone media port range configured on the Expressway. For more information, refer to the **Inbound (Internet > DMZ)** requirements in **Appendix 3: Firewall and NAT Settings** on page 52 of Cisco VCS Basic Configuration Control with Expressway Deployment Guide X8-5 if using Expressway 8.5. If using an earlier supported Expressway version, refer to the same section in the appropriate version of the guide on Cisco.com. **Note:** For outbound, all ports >1024 need to be opened.
WebEx client to WebEx Cloud	UDP ports 9000-9001*

*For a complete list of WebEx IP subnets, refer to article **WBX264**, in the WebEx Knowledge Base.

Note: On WebEx clients using UDP vs TCP, and customers should check their firewall setting to prevent UDP from being blocked.

IMPORTANT: Firewalls, ports and protocols that do deep packet inspection should not be used. Specifically, the stateful packet inspection used in Check Point Software Technologies, Inc. firewalls is incompatible with Cisco VCS Expressway and Expressway-E.

Network and Client Restrictions that Affect Video in the WebEx Client

- WebEx on PC or Mac will not be able to receive video if PC has a bit rate below 500Kbps, or too many applications open not leaving enough PC CPU or memory for receiving or sending video packets.
- WebEx clients on PC or Mac connect to WebEx datacenter using UDP if available or TCP if UDP is blocked. Optimal Video performance requires UDP. Customers should check with their security team to allow UDP ports for video where possible. Using TCP will prevent video in most cases, especially if using wifi network that is not optimized.
- Customers using Internet proxy in most cases will not be able to use UDP, which will cause video capacity limitations.

TIP: Within the WebEx PC client choose Meeting, Voice and Video Stats to view bit rate in use, and if UDP or TCP port in use to help in troubleshooting lose of video.

Understanding CMR Hybrid Scheduling Flow

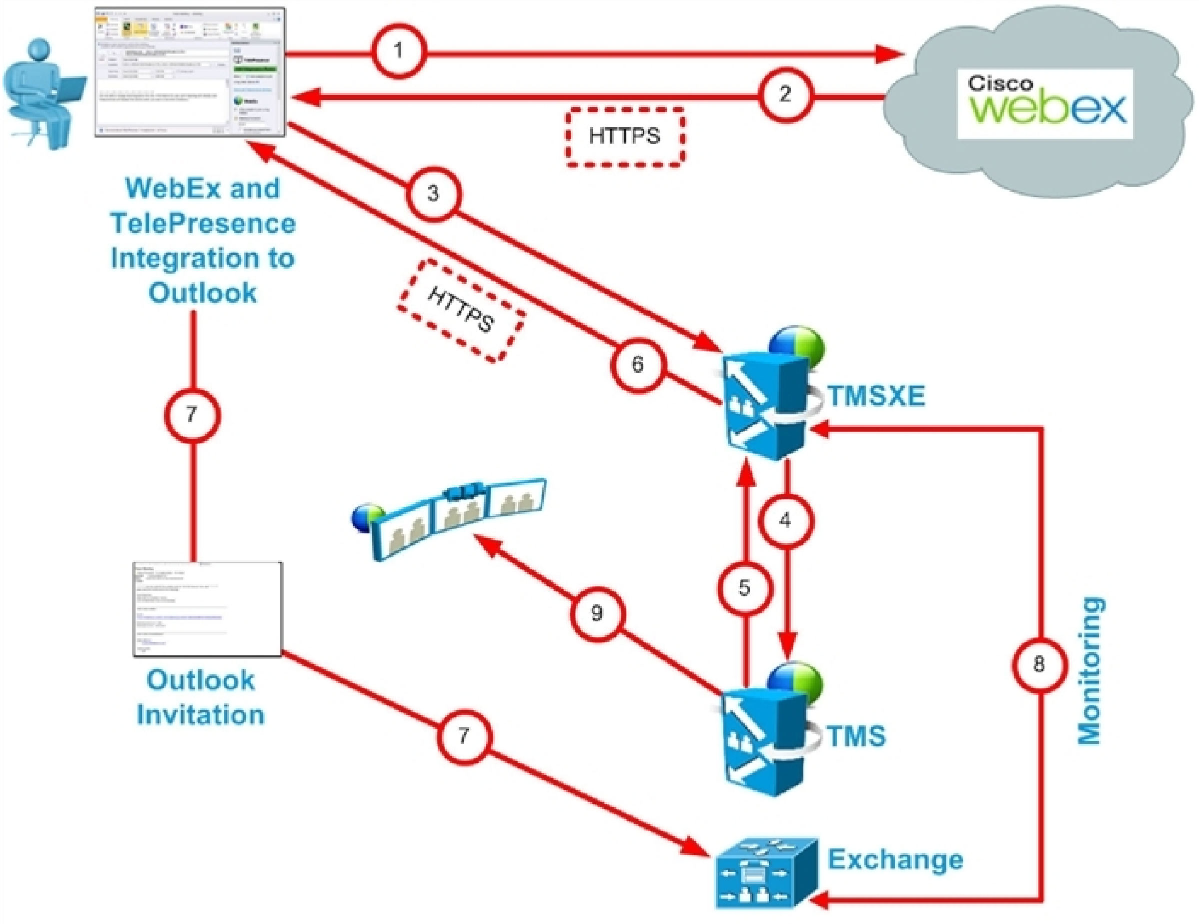
This section describes what takes place when a CMR Hybrid is scheduled using the following:

- Scheduling with the Cisco WebEx and TelePresence Integration to Outlook [p.31]
- Scheduling with the Cisco Smart Scheduler [p.33]
- Scheduling with the Cisco WebEx Scheduling Mailbox [p.35]

Note: Multiple deployments are possible at the same time. For example, when using Smart Scheduler, if Microsoft Exchange is deployed, the calendar of any rooms booked for a meeting is updated with the meeting details.

Scheduling with the Cisco WebEx and TelePresence Integration to Outlook

Figure 9: Cisco WebEx and TelePresence Integration to Outlook Scheduling Flow

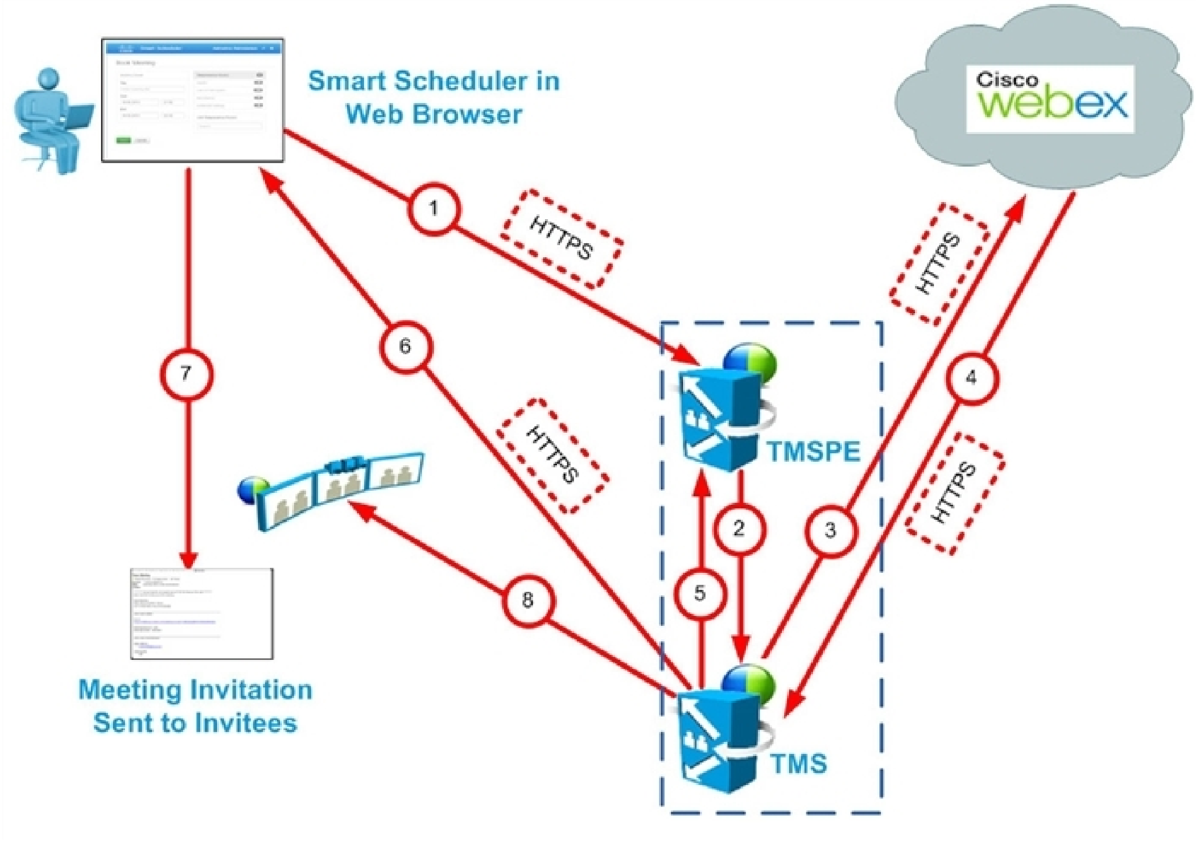


Cisco WebEx and TelePresence Integration to Outlook Scheduling Steps

Step #	Description
1	User books meeting with Cisco WebEx and TelePresence Integration to Outlook. Adds users Adds rooms Meeting request is sent to WebEx and books the WebEx portion of meeting.
2	WebEx responds with meeting information: Date and time of meeting Meeting subject Audio dial-in information If TSP audio, then the audio will contain additional info for the MCU to dial the TSP provider. SIP video and audio (if SIP audio) dial-in information for the bridge to dial into WebEx Meeting URL for participants to click
3	Cisco WebEx and TelePresence Integration to Outlook contacts TMSXE and does a booking request which includes the WebEx info from step 2.
4	TMSXE sends a booking request with the same information to TMS.
5	TMS confirms the meeting and returns the meeting details to TMSXE.
6	TMSXE sends the meeting confirmation to the Cisco WebEx and TelePresence Integration to Outlook.
7	Outlook invitation is sent back to Exchange to book the rooms and to also any added participants.
8	TMSXE monitors the room mailbox to make sure the rooms accept the meeting.
9	If user invited TelePresence rooms, TMS One-Button-to-Push information is sent to the TelePresence endpoints.

Scheduling with the Cisco Smart Scheduler

Figure 10: Cisco WebEx Smart Scheduler Scheduling Flow


Smart Scheduler in Web Browser
Cisco webex
1
HTTPS
HTTPS
6
7
HTTPS
4
HTTPS
TMSPE
2
3
5
8
Meeting Invitation Sent to Invitees
TMS

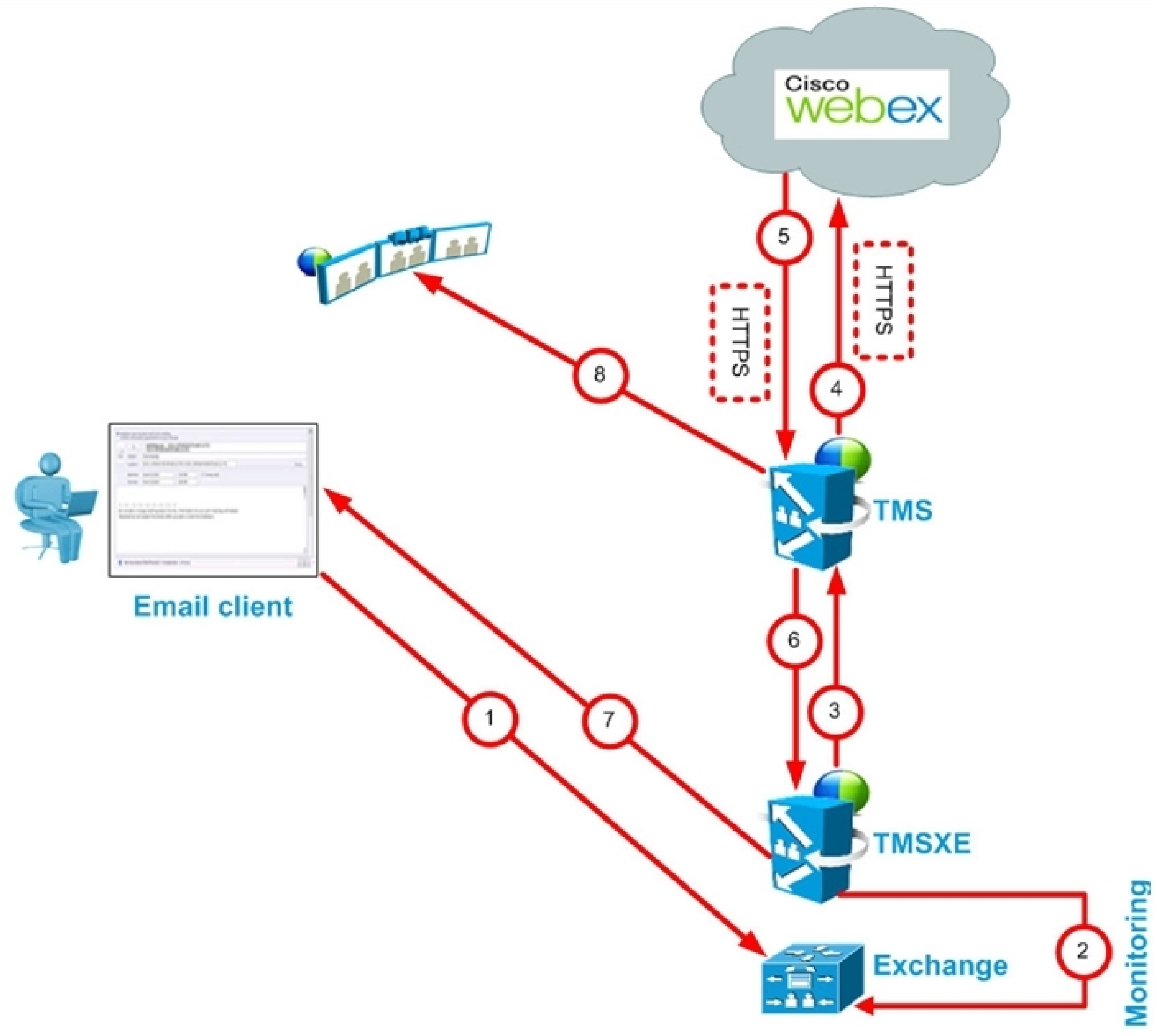
Cisco Smart Scheduler Scheduling Steps

Step #	Description
1	User books meeting with Smart Scheduler. Adds rooms Adds WebEx Clicks Save.
2	TMSPE sends a booking request to TMS.
3	TMS sends booking request to WebEx. WebEx books WebEx portion of meeting.

Step #	Description
4	WebEx sends meeting details in response to the booking request from TMS: Date/time of the meeting Meeting subject Audio dial-in information if TSP audio, then the audio will contain additional info for the MCU to dial the TSP provider. SIP video and audio (if SIP audio) dial-in information for the bridge to dial into WebEx Meeting URL for participants to click
5	TMS responds to TMSPE with booking confirmation information.
6	TMS sends confirmation email to user.
7	User sends meeting invitation with meeting details to invitees.
8	If user invited TelePresence rooms, TMS sends One-Button-to-Push information to the TelePresence endpoints.

Scheduling with the Cisco WebEx Scheduling Mailbox

Figure 11: Cisco WebEx Scheduling Mailbox Scheduling Flow



Cisco WebEx Scheduling Mailbox Scheduling Steps

Step #	Description
1	User books meeting in email/calendar client supported by Microsoft Exchange: Adds rooms Adds WebEx Scheduling Mailbox (e.g. webex@example.com) Adds participants Clicks Send Meeting request is sent to Exchange.
2	TMSXE monitors mailboxes for the rooms and the WebEx Scheduling Mailbox.

Step #	Description
3	TMSXE communicates with the booking API on TMS to request a WebEx-enabled meeting.
4	TMS requests WebEx to book the WebEx portion of the meeting.
5	WebEx sends meeting details in response to the booking request from TMS: Date/time of the meeting Meeting subject Audio dial-in information if TSP audio, then the audio will contain additional info for the MCU to dial the TSP provider. SIP video and audio (if SIP audio) dial-in information for the bridge to dial into WebEx Meeting URL for participants to click.
6	TMS responds to TMSXE with booking confirmation information.
7	TMSXE sends email confirmation to meeting organizer.
8	If user invited TelePresence rooms, TMS sends One-Button-to-Push information to the TelePresence endpoints.

Understanding CMR Hybrid Call Flow

This section describes the call flow of the following CMR Hybrid Meetings:

SIP Audio Call Flow

Figure 12: SIP Audio Call Flow

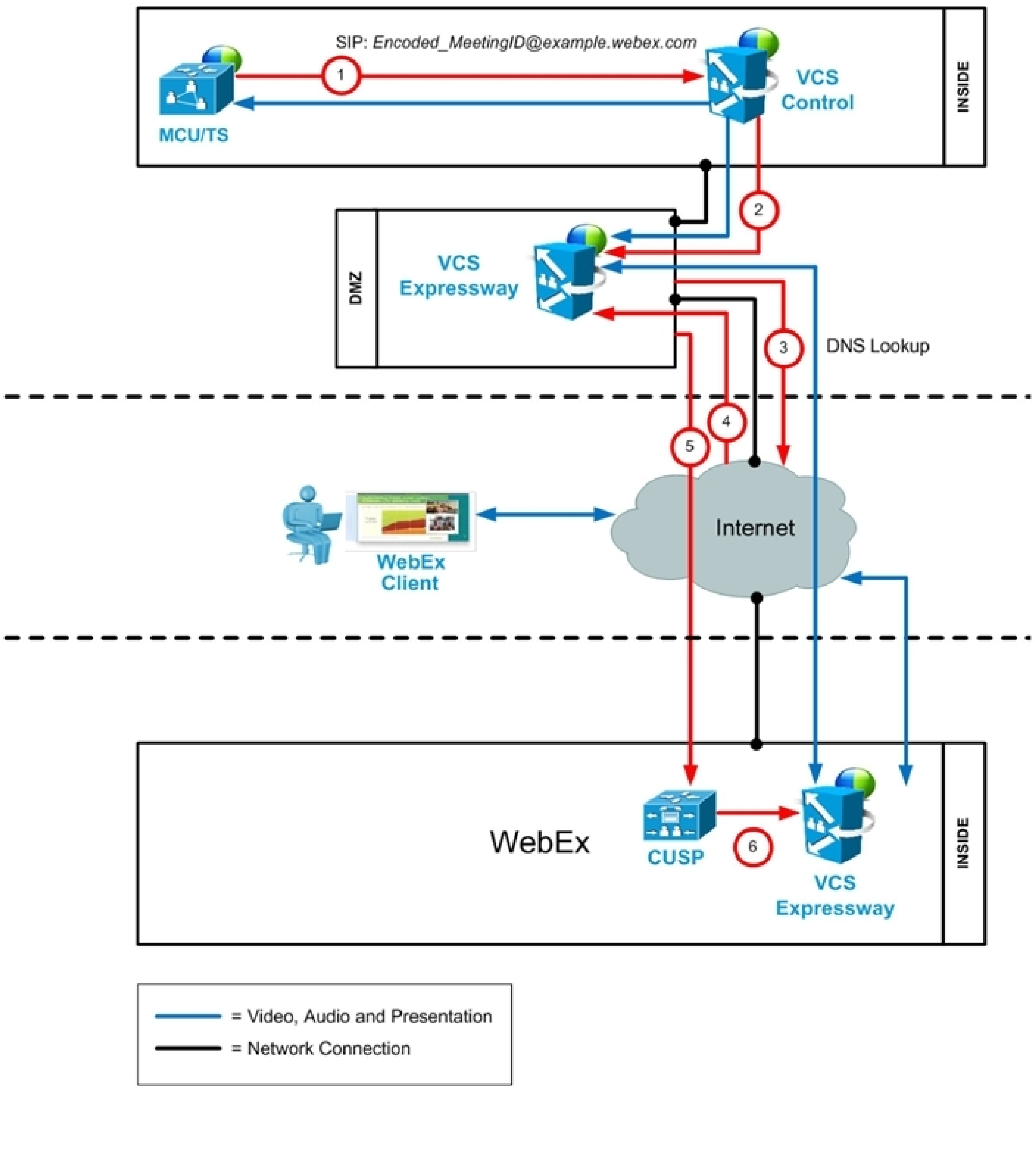


Table 4: SIP Audio Call Flow Steps

Step #	Description
1	MCU calls WebEx using SIP URI and the call is routed through Cisco VCS Control

Table 4: SIP Audio Call Flow Steps (continued)

Step #	Description
2	Cisco VCS Control sends call to VCS-E through the traversal zone.
3	Cisco VCS Expressway does a DNS lookup for example.webex.com.
4	DNS resolves example.webex.com to the CUSP servers.
5	Cisco VCS Expressway sends call to CUSP. This step is always encrypted (mandatory) (encryption is optional on previous steps). - Cisco VCS Expressway and the CUSP server verify each other's certificates.
6	CUSP forwards the call to Cisco VCS Expressway inside the WebEx dmz. - This leg is encrypted also (mandatory).
7	Media is connected. - Media is encrypted between the two Cisco VCS Expressways (across the Internet) - It is optional whether it is encrypted between the MCU and the Cisco VCS Expressway in the customer's site.

TSP Audio Call Flow with API Command to Unlock Waiting Room

Figure 13: TSP Audio Call Flow with API Command to Unlock Waiting Room

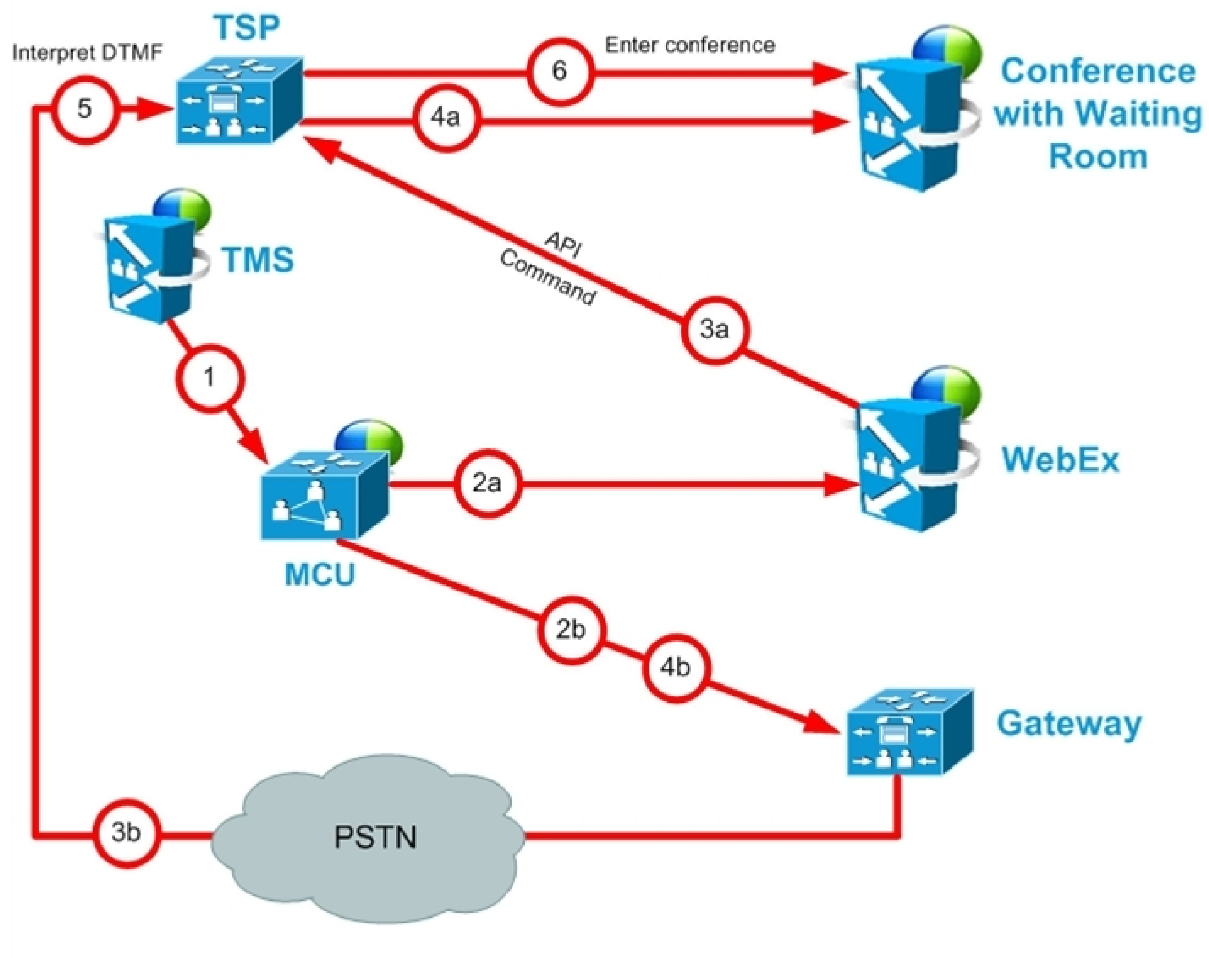


Table 5: TSP Audio Call Flow with API Command to Unlock Waiting Room Steps

Step #	Description
1	TMS starts the conference on MCU/TelePresence Server, providing it with the SIP URI, telephone number (if using PSTN audio) and DTMF String (if using PSTN audio) to dial into WebEx
2a	MCU/TelePresence Server dials WebEx via SIP. (refer to Understanding CMR Hybrid Call Flow [p.37] for details).
2b	At the same time as step 2a, MCU/TelePresence Server dials PSTN call-in number for WebEx.
3a	WebEx notifies TSP provider using API command to start the audio conference, and as part of that, WebEx tells the TSP provider that the conference type = telepresence and that it should unlock the waiting room.

Table 5: TSP Audio Call Flow with API Command to Unlock Waiting Room Steps (continued)

Step #	Description
3b	At the same time as step 3a, TSP provider prompts the MCU/TelePresence Server for the meeting access number.
4a	TSP provider unlocks waiting room, in response to step 3a.
4b	At the same time as step 4a, MCU/TelePresence Server sends DTMF tones it was prompted for in step 3b to TSP.
5	TSP provider receives the DTMF tones.
6	TSP provider places MCU/TelePresence Server into the audio conference.

TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host

Figure 14: TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host

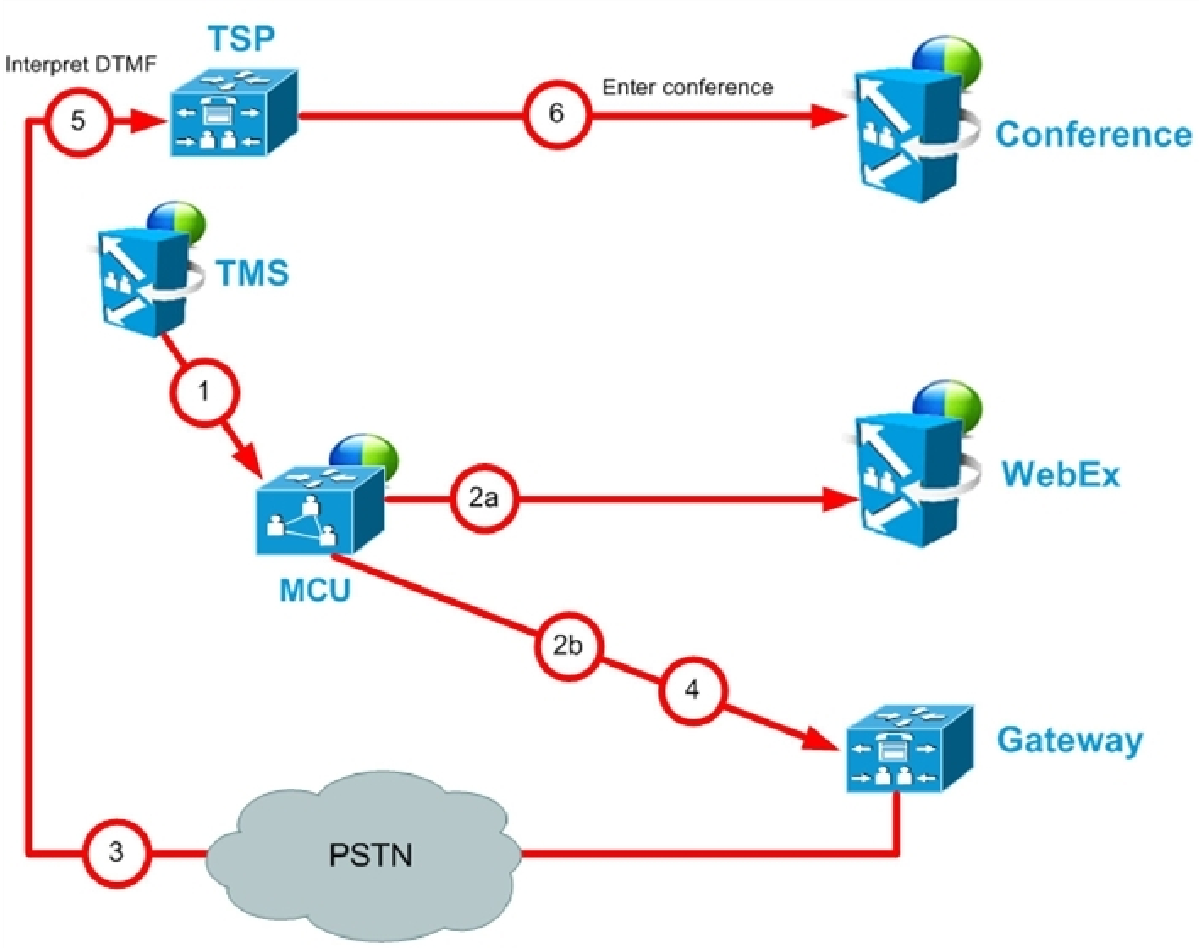


Table 6: TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host Steps

Step #	Description
1	TMS starts conference on MCU/TelePresence Server, providing it with the SIP URI, telephone# (if using PSTN audio) and DTMF String (if using PSTN audio) to dial into WebEx
2a	MCU/TelePresence Server dials webex via SIP. (refer to Understanding CMR Hybrid Call Flow [p.37] for details).
2b	At the same time as step 2a, MCU/TelePresence Server dials PSTN call-in number for WebEx.
3	TSP provider prompts the MCU/TelePresence Server for the meeting access number and host key.
4	MCU/TelePresence Server sends DTMF tones and host key it was prompted for in step 3.
5	TSP provider receives the DTMF tones.
6	TSP provider unlocks the waiting room and places the MCU/TelePresence Server into the audio conference.

WebEx Audio (PSTN) Call Flow

Figure 15: WebEx Audio (PSTN) Call Flow

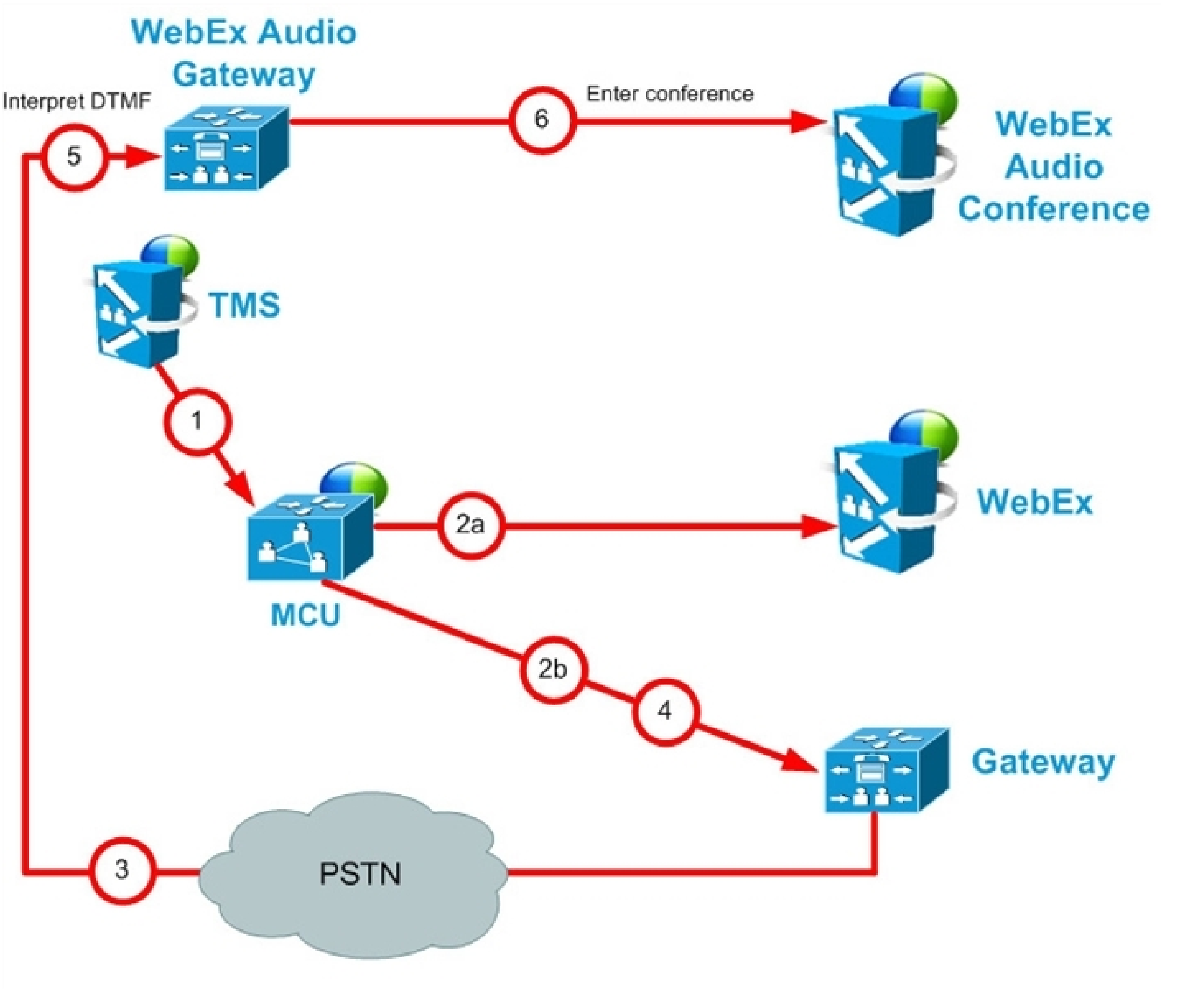


Table 7: WebEx Audio (PSTN) Call Flow Steps

Step #	Description
1	TMS starts conference on MCU, providing it with the SIP URI, telephone number and DTMF string to dial into WebEx.
2a	MCU dials WebEx via SIP. (refer back to Understanding CMR Hybrid Call Flow [p.37] for details).
2b	At the same time as step 2a, MCU dials PSTN call-in number for WebEx.
3	WebEx prompts the MCU for the meeting access number.
4	MCU sends DTMF tones it was prompted for in step 3 to TSP.
5	WebEx receives the DTMF tones.
6	WebEx places the MCU into the audio conference.

Configuration Checklist

First Published: June 23, 2014

This chapter describes items and configuration tasks required to deploy CMR Hybrid as a first-time deployment or upgrading an existing deployment. It contains the following sections:

Server and Site Access Checklist

Table 8: Information you must have before configuring CMR Hybridfor the first time.

What You Need	Description and Source	✓
WebEx Site URL	URL for the Cisco WebEx site. Provided by the Cisco WebEx Account Team. Example: **`https://example.webex.com/example`** See Configuring the Cisco WebEx Feature in Cisco TMS [p.99] for instructions.	
WebEx Site Hostname	Hostname of WebEx site used by the customer. Provided by the Cisco WebEx Account Team. Example: **`example.webex.com`** See Configuring Cisco TelePresence Management Suite [p.97] for instructions.	
WebEx Site Administration URL	Your unique address for accessing the Cisco WebEx Site Administration interface where you complete your initial Cisco WebEx setup configuration and manage and maintain your account after initial setup. This URL takes you directly to the WebEx Administration site. Provided by the Cisco WebEx Account Team. Example: **`https://example.webex.com/admin`** See Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.149] for instructions.	
Cisco WebEx Administrator username	Cisco WebEx Site Administrator account username. Provided by the Cisco WebEx Account Team. Example: **`webexAdmin`** See Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.149] for instructions.	
(Optional) Certificate pair, including public certificate and private key from TMS	Used to authenticate Cisco TMS to the WebEx cloud for meetings booked by users with WebEx accounts when Single Sign On (SSO) is enabled on TMS. When SSO is configured and a user schedules a WebEx-enabled meeting, the WebEx username in their Cisco TMS user profile is passed to the WebEx site to complete the booking. See Configuring Single Sign On in Cisco TMS [p.110] for instructions.	
Client/server certificate for Cisco VCS Expressway	Because the call leg between the Cisco VCS Expressway and the WebEx cloud must be encrypted, a valid client/server certificate is required for the SSL handshake to occur so that secure signaling and media can take place. See Configuring Cisco Expressway and TelePresence Video Communication Server [p.61] and Configuring Certificates on Cisco Expressway-E and Cisco VCS Expressway [p.68] for instructions.	

Configuration Task Checklist

You can choose the order in which you wish to configure Cisco TelePresence components for CMR Hybrid; the following order is only a suggestion, though you must complete all of the configuration steps in this checklist to enable the feature and Cisco TelePresence must be enabled before you can configure Cisco WebEx Site Administration.

1. Conference bridges:
   - Configuration Task Checklist [p.46]
   - Cisco TelePresence Server [p.47]
2. Call control:
   - Cisco TelePresence Video Communication Server [p.47]
   - Cisco TelePresence Management Suite Extension for Microsoft Exchange [p.48]
3. Scheduling:
   - Cisco TelePresence Management Suite [p.48]
   - Cisco TelePresence Management Suite Extension for Microsoft Exchange [p.48]
4. Audio:
   - Audio for CMR Hybrid [p.49]
5. WebEx site:
   - Cisco WebEx Site Administration [p.49]

Table 9: Checklist — Configuring CMR Hybrid on the MCU for the First Time

Go to: Configuring Cisco MCU and TelePresence Server [p.51]

Task	Detailed Instructions	✓
Configure SIP	Required Settings for MCU [p.53]	
Configure the Content Mode.	Required Settings for MCU [p.53]	
Configure the Video and Audio Codecs.	Required Settings for MCU [p.53]	
Configure the Automatic Content Handover.	Required Settings for MCU [p.53]	
Configure Optional Recommended Settings: ■ Automatically Make Content Channel Important ■ Outgoing Transcoded Codec ■ Adaptive Gain Control ■ Join and Leave Audio Notifications ■ Encryption	Recommended Settings for MCU [p.55]	

Cisco TelePresence Server

Table 10: Checklist — Configuring CMR Hybrid on TelePresence Server for the First Time

Go to: Configuring Cisco MCU and TelePresence Server [p.51]

Task	Detailed Instructions	✓
Configure SIP	Required Settings for TelePresence Server [p.57]	
Configure Locally Managed Mode	Required Settings for TelePresence Server [p.57]	
Configure the Automatic Content Handover.	Required Settings for TelePresence Server [p.57]	
Configure Optional Recommended Setting: Display Setting	Recommended Settings for TelePresence Server [p.58]	

Cisco TelePresence Video Communication Server

Table 11: Checklist — Configuring CMR Hybrid on Cisco TelePresence Video Communication Server for the First Time

Go to: Configuring Call Control [p.59]

Task	Detailed Instructions	✓
Create a New DNS Zone on Cisco VCS Expressway for WebEx ■ Create a new DNS zone ■ Turn on TLS Verify mode and enter TLS verify subject name. ■ Set up a search rule for the WebEx domain	Configuring Cisco Expressway and TelePresence Video Communication Server [p.61]	
Configure a valid Client/Server Certificate	Configuring Certificates on Cisco Expressway-E and Cisco VCS Expressway [p.68],	
Configuring Traversal Zones for MCUs with Encryption Enabled	Configuring Cisco Expressway and TelePresence Video Communication Server [p.61]	
If deploying with Unified CM: Configure a SIP trunk between Unified CM and Cisco VCS Control.	Configuring Cisco Unified Communications Manager [p.64]	

Cisco Unified Communications Manager

Table 12: Checklist — Configuring CMR Hybrid on Unified CM for the First Time

Go to: Configuring Call Control [p.59]

Task	Detailed Instructions	✓
Configure a SIP trunk between Unified CM and Cisco VCS Control.	Configuring Cisco Unified Communications Manager [p.64]	

Cisco TelePresence Management Suite

Checklist — Configuring CMR Hybrid on Cisco TMS for the First Time

Go to: Configuring Cisco TelePresence Management Suite [p.97]

Task	Detailed Instructions	✓
Enable the WebEx feature in Cisco TMS.	Configuring the Cisco WebEx Feature in Cisco TMS [p.99]	
Configure WebEx users in Cisco TMS.	Configuring WebEx Users in Cisco TMS [p.101]	
Configure Hybrid Content Mode for MCU in Cisco TMS.	Configuring Hybrid Content Mode for MCU in Cisco TMS [p.105]	

Cisco TelePresence Management Suite Extension for Microsoft Exchange

Complete the steps below if you want to deploy the feature of scheduling CMR Hybrid meetings using Microsoft Outlook. You have the option of configuring one or both of the following scheduling options:

- WebEx and TelePresence to Outlook
- WebEx Scheduling Mailbox

Table 13: Checklist — Configuring CMR Hybrid on Cisco TMSXE for the First Time

Go to: Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange [p.118]

Task	Detailed Instructions	✓
Configure TMSXE for scheduling with WebEx and TelePresence Integration to Microsoft Outlook.	Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook [p.122]	
Configure TMSXE for scheduling with WebEx Scheduling Mailbox.	Configuring Cisco TMSXE for the WebEx Scheduling Mailbox [p.126]	

Cisco TelePresence Management Suite Provisioning Extension

Complete the steps below if you want to deploy the feature of scheduling CMR Hybrid meetings using Smart Scheduler.

Table 14: Checklist — Configuring CMR Hybrid on Cisco TMSPE for the First Time

Task	Detailed Instructions	✓
Install and enable Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) on Cisco TMS.	Cisco TelePresence Management Suite Provisioning Extension Deployment Guide.	
Review additional prerequisites, and information about Cisco TMSPE and Smart Scheduler.	Configuring Cisco TelePresence Management Suite Provisioning Extension [p.128]	

Audio for CMR Hybrid

Table 15: Checklist — Configuring Audio for CMR Hybrid for the First Time

Go to: Configuring Audio [p.135]

Task	Detailed Instructions	✓
Configuring SIP Audio for Cisco Collaboration Meeting Rooms (CMR) Hybrid: ■ Configure the WebEx Site in Cisco TMS to Use SIP Audio. ■ Enable Hybrid Mode on the WebEx Site	Configuring SIP Audio for CMR Hybrid [p.137]	
Configuring PSTN Audio for Cisco Collaboration Meeting Rooms (CMR) Hybrid: ■ Configure the WebEx Site in Cisco TMS to Use PSTN Audio ■ Enable Hybrid Mode on the WebEx Site (Optional) ■ Configure PSTN Calls to Pass Through a PSTN gateway to WebEx	Configuring PSTN Audio for CMR Hybrid [p.139]	
(If applicable) Configure TSP audio for CMR Hybrid. ■ Configure the MACC Domain Index and Open TSP Meeting Room WebEx settings. ■ Configure the TSP dial string. ■ Configure how the conference is opened. ■ Configure TSP audio for the meeting organizer.	Configuring TSP Audio for CMR Hybrid [p.142]	

Cisco WebEx Site Administration

After WebEx provisions your site for CMR Hybrid, follow these steps.

Table 16: Checklist — Setting up Cisco WebEx Site Administration for the First Time

Go to: Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.149]

Required Task	Detailed Instructions	✓
Enable Cisco TelePresence Integration (MC only).	Configuring Cisco WebEx Site Administration for CMR Hybrid [p.150]	
(Recommended) Enable TelePresence options: ■ List TelePresence on calendar ■ Send invitation email to meeting host ■ Display toll-free number to attendees		
Set the Cisco TelePresence VOIP and video connection.		
Select the Cisco TelePresence PRO: Meeting Center TelePresence Session Type.	Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.150]	

Configuring Cisco MCU and TelePresence Server

First Published: June 23, 2014

Note: MCU software release 4.5 or later is required for Unified CM-centric deployments.

This chapter describes how to configure MCU and TelePresence Server for CMR Hybrid meetings. It contains the following sections:

Introduction

This chapter describes specific settings on both MCU and TelePresence Server that are required or recommended for use with CMR Hybrid meetings.

There are two deployment options for MCU and TelePresence Server:

- MCU and TelePresence Server trunked to Cisco Unified CM
- MCU and TelePresence Server registered to Cisco Expressway-C or Cisco VCS Control

In terms of user experience, the active speaker from TelePresence to MCU or TelePresence Server is shown to WebEx users and the active speaker from WebEx to MCU or TelePresence Server is shown to TelePresence. TelePresence Server, by default, using a feature called ActivePresence, displays a full screen view of the active speaker and up to nine additional TelePresence participants in a row at the bottom of the screen. MCU, by default displays a full screen view of the active speaker. For more information about the screen layout options available, refer to the TelePresence Server and MCU documentation.

Note: Only Cisco multiparty bridges, such as the Cisco TelePresence Server and Cisco TelePresence MCU, are supported for CMR Hybrid.

Required Settings for MCU

The following settings on MCU are required for CMR Hybrid:

- SIP [p.53]
- Content Mode [p.53]
- Video and Audio Codecs [p.53]
- Automatic Content Handover [p.54]
- Configuring the Default SIP Domain in MCU 4.5 for TSP Audio [p.54]

SIP

MCU calls to WebEx support SIP only. Make sure SIP is configured correctly on MCU. The call leg between MCU/TS,Cisco Unified CM, Cisco Expressway-C, Cisco VCS Control, Cisco Expressway-E, Cisco VCS Expressway and the WebEx cloud cannot be interworked.

Note: Refer to MCU help for more information on how to configure SIP.

Content Mode

In Hybrid mode, the incoming content stream is passed through, giving the best possible quality to HD endpoints and it is also decoded and used to create a second, lower resolution stream for anyone who cannot receive the passthrough stream (SD endpoints). This uses up a video port but ensures that users get the advantages both of transcoding and passthrough.

If content mode is set to Passthrough, a single video stream is sent to everyone in the meeting. If all participants are HD endpoints, they receive the best possible quality. However, if one or more participants can only receive SD video, then all participants receive SD video.

Though Content Mode can be set on the MCU, Cisco recommends customers to set it using TMS.

To configure hybrid content mode for MCU in TMS, refer to:

Configuring Hybrid Content Mode for MCU in Cisco TMS [p.105].

Video and Audio Codecs

WebEx requires H.264 for video and content and G.711 and G.722 for audio.

To set video and audio codecs in MCU, do the following:

1. Log into the MCU.
2. Click **Settings**.
3. The Settings page appears with the Conferences tab displayed.
4. In the Advanced Settings section make sure **H.264** is checked for the following:
5.
   - Video codecs from MCU
   - Video codecs to MCU
6. In the Advanced Settings section make sure **G.711** and **G.722** are checked for the following:

- Audio codecs from MCU
- Audio codecs to MCU

7. At the bottom of the page, click **Apply changes**.

Automatic Content Handover

This feature must be enabled for TelePresence endpoints to share during a CMR Hybrid meeting.

To enable Automatic Content Handover in MCU, do the following:

1. Log into the MCU.
2. Click **Settings**.
3. The Settings page appears with the Conferences tab displayed.
4. Click the **Content** tab.
5. For Automatic content handover, select **Enabled**.
6. At the bottom of the page, click **Apply changes**.

Configuring the Default SIP Domain in MCU 4.5 for TSP Audio

With MCU release 4.5, in a deployment that uses TSP audio, it is required to configure the default SIP domain. This is only required for TSP audio.

When TMS instructs MCU to dial a number, it provides the number without the @*domain* portion. Because the domain is required for the call to be successful, MCU must automatically add the domain on to the number it dials.

To configure the Default SIP Domain in MCU release 4.5, do the following:

1. Log into the MCU.
2. Click **Settings**.
3. The Settings page appears.
4. Click the **SIP** tab.
5. For Outbound call configuration, select **Use Trunk**.
6. For Outbound address, enter the hostname or IP address of the trunk destination.
7. For Outbound domain, enter the domain of the trunk destination.

For more information, refer to the MCU online help.

Recommended Settings for MCU

For best results with CMR Hybrid, Cisco recommends configuring the following settings in MCU:

- Automatically Make Content Channel Important [p.55]
- Outgoing Transcoded Codec [p.55]
- Adaptive Gain Control [p.55]
- Join and Leave Audio Notifications [p.56]
- Encryption [p.56]

Automatically Make Content Channel Important

Cisco recommends setting the conference settings to automatically make the content channel important. Any new content channel in a conference will be treated as important and displayed prominently to all participants who see the content channel in their conference layout.

To enable automatically making the content channel important, do the following:

1. Log into the MCU.
2. Click **Settings**.
3. The Settings page appears with the Conferences tab displayed.
4. In the Advanced Settings section, check **Automatically make content channel important**.
5. At the bottom of the page, click **Apply changes**.

Outgoing Transcoded Codec

Cisco recommends setting the outgoing transcoded codec to H.264. This makes the MCU use the H.264 video codec for outgoing transcoded content channels.

To set the outgoing transcoded codec to H.264, do the following:

1. Log into the MCU.
2. Click **Conferences** at the top of the page.
3. The Conferences page appears with the Conference list tab displayed.
4. Click the **Templates** tab.
5. The Conference Templates page appears.
6. Click the link for **Top level**.
7. The Top level template configuration page appears.
8. In the Content section, using the Outgoing transcoded codec menu, select **H.264**.
9. At the bottom of the page, click **Apply changes**.

Adaptive Gain Control

Cisco recommends setting adaptive gain control on join to be enabled. Adaptive Gain Control (AGC) alters the gain of each participant's audio so that all participants have a consistent volume level.

To set the adaptive gain control on join to be enabled, do the following:

1. Log into the MCU.
2. Click **Conferences** at the top of the page.
3. The Conferences page appears with the Conference list tab displayed.
4. Click the **Templates** tab.
5. The Conference Templates page appears.
6. Click the link for **Top level**.
7. The Top level template configuration page appears.
8. In the Parameters section, using the Adaptive Gain Control on join menu, select **Enabled**.
9. At the bottom of the page, click **Apply changes**.

Join and Leave Audio Notifications

This setting controls different aspects of sounds that can occur during a meeting. One setting to be aware of for CMR Hybrid meetings is Join and Leave Notifications, which are audible messages indicating when other participants join and leave the meeting. By default, these are enabled (checked).

WebEx also has join and leave notifications that are independent of those set in MCU. If the notifications are enabled on both MCU and WebEx, notifications will be heard for each participant joining and leaving the meeting on the MCU side and for participants on the WebEx side. As a result, you may want to disable the join and leaving notifications in MCU and/or WebEx.

To disable the join and leave audio notifications in MCU, do the following:

1. Log into the MCU.
2. Click **Settings**.
3. The Settings page appears with the Conferences tab displayed.
4. In the Conference Settings section, for Audio Notifications, uncheck **Join and leave indications**.
5. At the bottom of the page, click **Apply changes**.

Encryption

Cisco recommends that on MCUs with an encryption key, that the conference settings are configured to optionally encrypt the media. If encryption is set to require encryption of all media, then the main and content video sent to WebEx will be merged into a single stream and treated as a participant.

To set encryption to optional, do the following:

1. Log into the MCU.
2. Click **Conferences** at the top of the page.
3. The Conferences page appears with the Conference list tab displayed.
4. Click the **Templates** tab.
5. The Conference Templates page appears.
6. Click the link for **Top level**.
7. The Top level template configuration page appears.
8. In the Parameters section, using the Encryption menu, select **Optional**.
9. At the bottom of the page, click **Apply changes**.

Required Settings for TelePresence Server

The following setting in TelePresence Server is required for CMR Hybrid:

- SIP [p.57]
- Locally Managed Mode [p.57]
- Automatic Content Handover [p.57]

For more information about TelePresence Server software, refer to the following link:

http://www.cisco.com/en/US/products/ps11339/prod_release_notes_list.html

SIP

TelePresence Server calls to WebEx support SIP only. Make sure SIP is configured correctly on TelePresence Server.

Note: Refer to the TelePresence Server help for more information on how to configure SIP.

Locally Managed Mode

For TMS to control the TelePresence Server, the TelePresence Server must be set in locally managed mode. To set the operation mode, do the following.

To enable locally managed mode in TelePresence Server, do the following:

1. Log into the TelePresence Server.
2. Go to **Configuration** > **Operation mode**.
3. The Operation mode page appears.
4. Using the Operation mode menu, select **Locally managed**.
5. At the bottom of the page, click **Apply changes**.

Automatic Content Handover

This feature must be enabled for TelePresence endpoints to share during a CMR Hybrid meeting.

Note: This applies to hardware-based TelePresence Servers only. For TelePresence Server on Virtual Machine in remotely-managed mode, it is enabled automatically through the Conductor API.

To enable Automatic Content Handover in TelePresence Server, do the following:

1. Log into the TelePresence Server.
2. Go to **Configuration** > **System Settings**.
3. The System Settings page appears.
4. Make sure **Automatic content handover** is checked.
5. At the bottom of the page, click **Apply changes**.

Recommended Settings for TelePresence Server

For best results with CMR Hybrid, Cisco recommends the following setting on TelePresence Server:

- Display Setting [p.58]

Display Setting

Cisco recommends the display setting in TelePresence Server to be set to full screen, so that WebEx video can be shown full size on a multiscreen endpoint.

Note: This applies to hardware-based TelePresence Servers only. For TelePresence Server on Virtual Machine in remotely-managed mode, it is enabled automatically through the Conductor API.

To enable full screen display in TelePresence Server, do the following:

1. Log into TelePresence Server.
2. Go to **Configuration > Default Endpoint Settings**.
3. In the Display section, for Full screen view of single-screen endpoints, select *Allowed*.
4. At the bottom of the page, click **Apply changes**.

Configuring Call Control

First Published: June 23, 2014

This chapter describes how to configure call control for meetings.

Introduction

To begin using CMR Hybrid, you must configure the call control product(s) used in your video network.

There are four possible call control scenarios:

- Cisco Cisco Unified Communications Manager with Cisco Expressway-C and Cisco Expressway-E. Endpoints are registered and bridges are trunked to Unified CM only.
- Cisco VCS Control and Cisco VCS Expressway
  Endpoints are registered to Cisco VCS Control and/or Cisco VCS Expressway only and bridges are registered to Cisco VCS Control only.
- Cisco Unified Communications Manager with Cisco VCS Control and Cisco VCS Expressway
  Endpoints are registered to Unified CM only and bridges are registered to Cisco VCS Control only.
- Cisco VCS Control and Cisco VCS Expressway with Unified CM
  Endpoints are registered to Cisco VCS Control/Expressway and Unified CMonly and bridges are registered to Cisco VCS Control only.

Note: Using Unified CM as the call control solution requires either Cisco Expressway-C and Cisco Expressway-E or Cisco VCS Control and Cisco VCS Expressway to be deployed in order to communicate with WebEx, regardless of whether endpoints are registered to Unified CM or Cisco VCS.

Configuring Cisco Expressway and TelePresence Video Communication Server

The following section describes the steps required for configuring Cisco Expressway and Cisco TelePresence Video Communication Server for CMR Hybrid.

This section describes the following tasks:

Note: The procedures that follow apply to both VCS and Expressway products. Any step that refers to VCS Control also applies to Expressway-C. Likewise, any step that refers to VCS Expressway, also applies to Expressway-E.

Prerequisites

To configure WebEx in Cisco VCS or Expressway, the following are required:

- Cisco TelePresence Video Communication Server (Cisco VCS) must be running firmware X7.2.3 or a later release.
- **Note:** Customers using Static NAT on VCS Expressway X7.2.3 are highly recommended to not upgrade to X8.1 or X8.2 due to a defect that will cause the media part of a call to fail. If you are already using Static NAT with X8.1 or X8.2, refer to the recommended workarounds in Configuring Certificates on Cisco Expressway-E and Cisco VCS Expressway.
- Endpoints in the network are registered to Cisco VCS Control or Expressway and/or Unified CM

  Note: If endpoints are registered to Unified CM, you must configure a SIP trunk between Unified CM and Cisco VCS Control. For more information, refer to Configuring Cisco Unified Communications Manager [p.64].
- Cisco VCS Expressway must be assigned a static IP address
- Firewall must have port 5061 open to allow access to Cisco VCS Expressway
  - **If this port is not configured correctly, calls will not take place correctly.**
  - **IMPORTANT**: Stateful packet inspection used in Check Point Software Technologies, Inc. firewalls is incompatible with Cisco VCS Expressway and Expressway-E.
  - As a result, it is highly recommended to disable SIP and H.323 application layer gateways on routers/firewalls carrying network traffic to or from a VCS Expressway or Expressway-E, because, when these are enabled they can negatively affect the built-in firewall/NAT traversal functionality of the VCS
- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network
- Cisco VCS Control is in the private network
- Cisco VCS Expressway is in the DMZ and has access to the Internet

- Set zones and pipes appropriately (according to your network's requirements) to allow a minimum of 2-4 Mbps for WebEx calls. For more information about bandwidth controls, please refer to the Cisco VCS Administrator Guide at:
  http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/admin_guide/Cisco_VCS_Administrator_Guide_X7-2.pdf
- If endpoints are registered to Cisco VCS Control, it must be configured as the SIP Registrar/H.323 gatekeeper.
  In order for CMR Hybrid to work with endpoints registered to Cisco VCS Control, it is required to set up a Cisco VCS Control as a SIP registrar, enabling it to register SIP devices and route calls to them. Cisco VCS Control has the capability to be both an H.323 gatekeeper and a SIP registrar.
  Configuring Cisco VCS Control as a SIP registrar is done by configuring one or more SIP domains. The Cisco VCS Control will act as a SIP Registrar and Presence Server for these domains, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes these domains.
  For details on how to configure SIP domains in Cisco VCS Control, refer to the "Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide" at:
  https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf
- Intercompany TelePresence participants: If you want to allow participants from another company to be able to join via TelePresence, you must have a valid SIP SRV (secure SIP), non-secure SIP SRV or multiple SIP and H323 SRV records in place that resolve to the Cisco VCS Expressway for your configured SIP Domain so TelePresence participants can route to your Cisco VCS Expressway.

Creating a New DNS Zone on Cisco Expressway-E or VCS Expressway for WebEx

Connection to the WebEx cloud uses a new DNS zone, that needs to be configured on the Cisco VCS Expressway.

To configure the Expressway-E or Cisco VCS Expressway for CMR Hybrid, do the following:

1. Create a new DNS zone:
   a. Set H.323 to **Off**.
   b. Set SIP Media encryption mode to **Force encrypted**.
   c. Turn on TLS Verify mode.
   d. In the TLS verify subject name field, enter **sip.webex.com**.
   e. Click **Create Zone**.
2. Set up a search rule with a higher priority than the search rule for the existing DNS zone (lower number priority) for the domain of WebEx.
   The following configuration is required:
   - Protocol: **SIP**
   - 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 Created for WebEx>**
   - State: **Enabled**

For details on how to create and set up search rules for a DNS zone, refer to the "Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide" at: https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-1.pdf.

3. Configure a valid Client/Server Certificate for your company. Typically the CName of the certificate is the routable domain to your company's Cisco VCS Expressway. It must be a CA-level certificate name issued by a public CA that is supported by WebEx. For a list of supported public CAs, see the list below.

   Note: Self-signed certificates are NOT supported.

For a list of supported certificates and details on how to configure a certificate on Cisco VCS Expressway, refer to: Configuring Certificates on Cisco Expressway-E and Cisco VCS Expressway [p.68].

Configuring Traversal Zones for MCUs with Encryption Enabled

This section details the configuration necessary in VCS to support MCUs that have encryption enabled (the default setting).

If you choose not to do the following configuration, MCUs with encryption enabled will deliver the presentation content in the main video channel, instead of a separate stream.

Note: In the following procedure, tasks for VCS Control are the same as for Expressway-C and tasks for Expressway-E or the same as for VCS Expressway.

To support MCUs that have encryption enabled, do the following

1. Set up a new traversal client zone from Cisco VCS Control to Cisco VCS Expressway

   Note: Make sure the new zone uses a different port number.

2. Configure the media encryption setting on the traversal client to be **Force unencrypted** or **Best effort**.
3. On Cisco VCS Expressway, set up a new traversal server zone that connects to the Cisco VCS Control traversal zone set up in the previous step.
4. In this new Cisco VCS Expressway traversal server zone, set media encryption to **Force unencrypted**.
5. On Cisco VCS Control set up a search rule (at higher priority than the search rule that uses the default traversal zone) that matches WebEx traffic e.g. match = .*@example.webex.com

Note: The above configuration ensures that whether the MCU encryption is enabled or not, that the video and the presentation stay on separate channels. It also ensures the content from WebEx is not encrypted when sent to the MCU (even though it is encrypted across the internet).

Configuring Cisco Unified Communications Manager

The following section describes the steps required for configuring Cisco Unified Communications Manager (Unified CM) for CMR Hybrid. This configuration also supports deployments where endpoints are registered to Unified CM only or both Unified CM and Cisco VCS Control/Cisco VCS Expressway.

This section describes the following tasks:

Prerequisites

To configure WebEx in Cisco Unified Communications Manager (Unified CM), the following are required:

- Unified CM 9.1(2) or 10.5.
- Endpoints in the network are registered to Unified CM
- Conferencing Bridge(s) to be used (MCU or Cisco TelePresence Server) are already operational within the network and trunked to Unified CM or registered to VCS
- Cisco Expressway-C or Cisco VCS Control is deployed in the private network
- To ensure optimum SIP audio and video connectivity between MCU and TelePresence Server and the WebEx cloud, it is recommended to set region to permit a minimum of 2-4 Mbps.
- Cisco Expressway-E or Cisco VCS Expressway is configured with the DNS zone.

Configuring a SIP Trunk Between Unified CM and Cisco Expressway-C or Cisco VCS Control

This section describes how to configure the Cisco Expressway Series X8.1 or later or Cisco TelePresence Video Communication Server (Cisco VCS) version X.7.2.2 later and Cisco Unified Communications Manager (Unified CM versions 9.1.2 or 10.5) to interwork via a SIP trunk.

This is required for endpoints registered to Unified CM to participate in a Cisco Collaboration Meeting Rooms (CMR) Hybrid meeting and to call endpoints registered to Cisco VCS Control. In addition, make sure that the Unified CM neighbor zone in Cisco VCS is configured with BFCP enabled.

The configuration steps are detailed in the Cisco Unified Communications Manager with Cisco VCS Deployment Guides at the following locations:

For Unified CM 9.x or later and VCS X7.2 or later:

Cisco VCS and CUCM Deployment Guide (CUCM 8,9 and X7.2)

For Unified CM 9.x or later and VCS X8.1 or later:

Cisco VCS and CUCM Deployment Guide (CUCM 8,9 and X8.1)

For Unified CM 9.x or later and Expressway X8.1 or later:

[Cisco Expressway and CUCM via SIP Trunk Deployment Guide (CUCM 8,9 and X8.1)]

Configuring Early Offer for SIP Messaging

Configuring Early Offer is only required for a Unified CM-centric deployment, where bridges are trunked and endpoints are registered to Unified CM.

With Early Offer, the session initiator sends its capabilities in the SIP Invite and the called device chooses the preferred codec. Cisco recommends that all SIP trunks which carry TelePresence calls are configured for Early Offer.

Additionally, Early Offer is required from any direct scheduled bridges to Cisco Expressway or Cisco VCS to support CMR Hybrid calls. The entire path from the calling device to the service must be configured to support Early Offer.

Cisco VCS-centric deployments always run in Early Offer mode and this section is only relevant to Unified CM-centric deployments. It provides the recommended approach for configuring outbound trunks as Early Offer.

Note: The default configuration for Unified CM trunks is **Delayed Offer**.

All trunks between the following Optimized Conferencing elements should be enabled for Early Offer. No media termination point (MTP) resources should be made available to these trunks, directly or indirectly:

- Unified CM to Cisco Expressway-C
- Unified CM to Cisco VCS Control
- Unified CM to TelePresence Server
- Unified CM to MCU
- Unified CM to Unified CM trunks which carry traffic originating from a TelePresence endpoint and any of the network elements listed above should also be enabled for Early Offer, with no media termination point (MTP) resources. For example, in a call flow scenario of EX90 >> UCM1 >> UCM2 >> Conductor >> TelePresence Server, the trunk between UCM1 >> UCM2 and the trunk between UCM2 >> Conductor should be enabled for Early Offer.

To restrict the use of MTPs, all MTP resources should be removed from all Session Management Edition (SME) clusters, and all MTP resources on Unified CM clusters should be placed in Media Resource Groups that are inaccessible both to TelePresence endpoints and to SIP trunks carrying TelePresence traffic.

Some specific points apply in various deployment scenarios:

Scenario 1. Configuring Early Offer in a single Unified CM system

Conference bridges are connected to the Unified CM, with Unified CM trunked to the Cisco Expressway. Endpoints are registered to the Unified CM. In this scenario the following trunks must be configured for Early Offer:

- Unified CM to Cisco Expressway-C.

Scenario 2. Configuring Early Offer in a multi-cluster system

One or more Unified CM SME clusters with connected leaf Unified CM clusters. The conference bridges are connected to the Unified CM SME. The Unified CM SME is trunked to the Cisco Expressway-C. In this scenario the following trunks must be configured for Early Offer:

- Unified CM SME to Cisco Expressway-C.

Note: In multi-cluster systems with three or more clusters, where one Unified CM cluster is a dedicated Unified CM SME, endpoints never register to the Unified CM SME but always to a leaf Unified CM cluster.

Scenario 3. Configuring Early Offer in a multi-cluster system

One or more SME clusters with connected leaf Unified CM clusters. The conference bridges are connected to the leaf cluster(s). A single trunk connects the SME to the Cisco Expressway-C. In this scenario the following trunks must be configured for Early Offer:

- Unified CM SME to Cisco Expressway-C.
- Leaf Unified CM clusters to the Unified CM SME.

Configuring Early Offer (and fallback to Delayed Offer) for SIP trunks

1. For each trunk, do one of the following depending on your Unified CM version:
   - For Unified CM Version 9.1(2) systems, enable the **Early Offer support for voice and video calls (insert MTP if needed)**.
   - For Unified CM Version 10.5 systems, in the **Early Offer support for voice and video calls** dropdown, select Best Effort (*no MTP inserted*).
2. Remove all MTP resources from the following elements:
   a. SME clusters (in the case of Unified CM SME deployments).
   b. All TelePresence endpoints and SIP trunks on all Unified CM clusters.
3. Set **SIP Trunk DTMF Signaling Method** to RFC 2833 (the default).
4. Enable the **Accept Audio Codec Preference in Received Offer** option on the following elements:
   a. All SME SIP trunks (in the case of Unified CM SME deployments).
   b. All SIP trunks that carry TelePresence calls on all Unified CM clusters.

Fallback to Delayed Offer

For outgoing calls, the default settings provide for automatic fallback to Delayed Offer in cases where no MTP resource exists. Without fallback, issues may arise in non-Optimized Conferencing areas of the network. For incoming calls, Early Offer is supported with no requirement for MTP resources.

Endpoints

Any TelePresence endpoints registered to Unified CM should be configured with a Media Resource Group List (MRGL) that does not contain any MTP resources. So that when the endpoints place a call that traverses one of the above trunk types an MTP will not be available within the MRGL of the endpoint.

Configuring a Routing Rule for Bridges Trunked to Unified CM

For Unified CM-centric deployments, it is required to set up a routing rule for any MCU or TelePresence Server trunked to Unified CM.

If your MCU or TelePresence Server is trunked to Unified CM, it will dial a long string of characters at your CMR Hybrid site (example: *yoursite.webex.com*)

To ensure calls are routed correctly, set up a SIP routing pattern in Unified CM for your site to route to the SIP trunk for Expressway-C. For details, refer to the Unified CM documentation.

Also, make sure that the trunk for each MCU or TelePresence Server trunked to Unified CM has Early Offer enabled, as described in Configuring a Routing Rule for Bridges Trunked to Unified CM [p.66] .

Configuring Certificates on Cisco Expressway-E and Cisco VCS Expressway

First Published: June 23, 2014

This chapter describes the best practices for configuring certificates on Cisco Expressway-E and Cisco VCS Expressway, and contains the following sections:

Introduction

There are three parts to the configuration:

- Generating a certificate signing request (CSR)
- Installing the SSL Server Certificate on the Cisco VCS Expressway
- Installing and stacking the Trusted CA List on the Cisco VCS Expressway

Cisco VCS Expressway X7.2.3, Cisco Expressway-E or Cisco VCS ExpresswayX8.1 or later are supported. Only version X8.1 or later is supported with a Unified CM-centric deployment.

There are important differences in how each is configured, which are noted in the procedures that follow.

NOTE: Customers using Static NAT on VCS Expressway X7.2.3 are highly recommended to not upgrade to X8.1 or X8.2. If you are using Static NAT with Expressway-E or VCS Expressway X8.1 or X8.2, refer to the recommended workarounds in Cisco Expressway-E and VCS Expressway X8.1 and X8.2 Encryption Issue and Workarounds [p.69].

Cisco Expressway-E and VCS Expressway X8.1 and X8.2 Encryption Issue and Workarounds

There is an issue with the Encrypt on Behalf feature in Expressway-E X8.1 or X8.2 and VCS Expressway X8.1 or X8.2 when using Static NAT. Because X8.1 and X8.2 use the **Ethernet 2** IP address for the media part in SDP, the media part of calls will fail. (Caveat ID: CSCum90139). Customers using Static NAT on their VCS Expressways running X7.2.3 are urged not to upgrade to X8.1 or X8.2 until a maintenance release fixes this issue.

If you are using Static NAT on Expressway-E or VCS Expressway X8.1 or X8.2, Cisco recommends one of the following workarounds:

- Downgrade VCS Expressway to X7.2.3.
- Reconfigure Expressway-E or VCS Expressway X8.1 or X8.2 to not use Static NAT.
- Use Expressway-C or VCS Control to Encrypt on Behalf instead of VCS Expressway.

To use Expressway-C or VCS Control to encrypt on behalf, do the following:

1. On MCU turn Encryption **OFF** for all conferences.
2. On Expressway-C or VCS Control, change the dedicated WebEx Traversal zone to **Force Encrypted**.
3. On Expressway-E or VCS Expressway, change the dedicated WebEx DNS zone to **Encryption Auto**.

Videos Available

This entire configuration process for Cisco VCS Expressway X7.2.3 is also described and demonstrated in the following video series:

Configuring Certificates on Cisco VCS Expressway for CMR Hybrid

Supported Certificates

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

NOTE: Self-signed certificates are NOT supported.

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[1]
- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- GlobalSign Root R1

Note: With the GlobalSign Root certificate, it is possible to be assigned R2 or R3 (or others, in the future). If assigned one of these, you must rekey the certificate to R1. Contact GlobalSign for assistance.

- 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://kb.webex.com/WBX83490.

CAUTION: Wildcard certificates are not supported on Cisco VCS Expressway.

[1] To use a certificate generated by entrust_2048_ca with Cisco VCS Expressway 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).

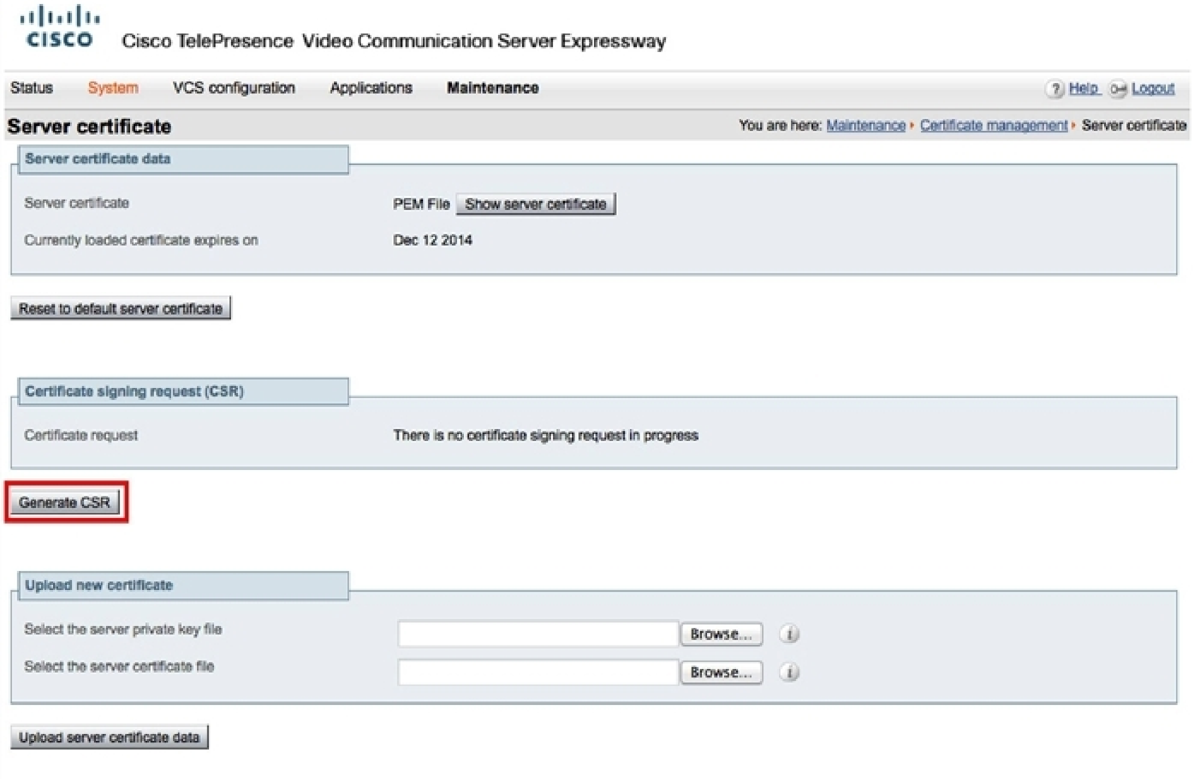
Generating a Certificate Signing Request (CSR)

To generate a certificate signing request, do the following:

In Cisco Expressway-E or Cisco VCS Expressway:

- X8.1, go to **Maintenance > Security certificates > Server certificate**.
- X7.2.3, go to **Maintenance > Certificate management > Server certificate**.

1. Click **Generate CSR**.


Cisco TelePresence Video Communication Server Expressway
Status
System
VCS configuration
Applications
Maintenance
Help
Logout
Show server certificate
Reset to default server certificate
Generate CSR
Browse...
Browse...
Upload server certificate data

Server certificate

You are here: Maintenance ▸ Certificate management ▸ Server certificate

Server certificate data

Server certificate: PEM File

Currently loaded certificate expires on: Dec 12 2014

Certificate signing request (CSR)

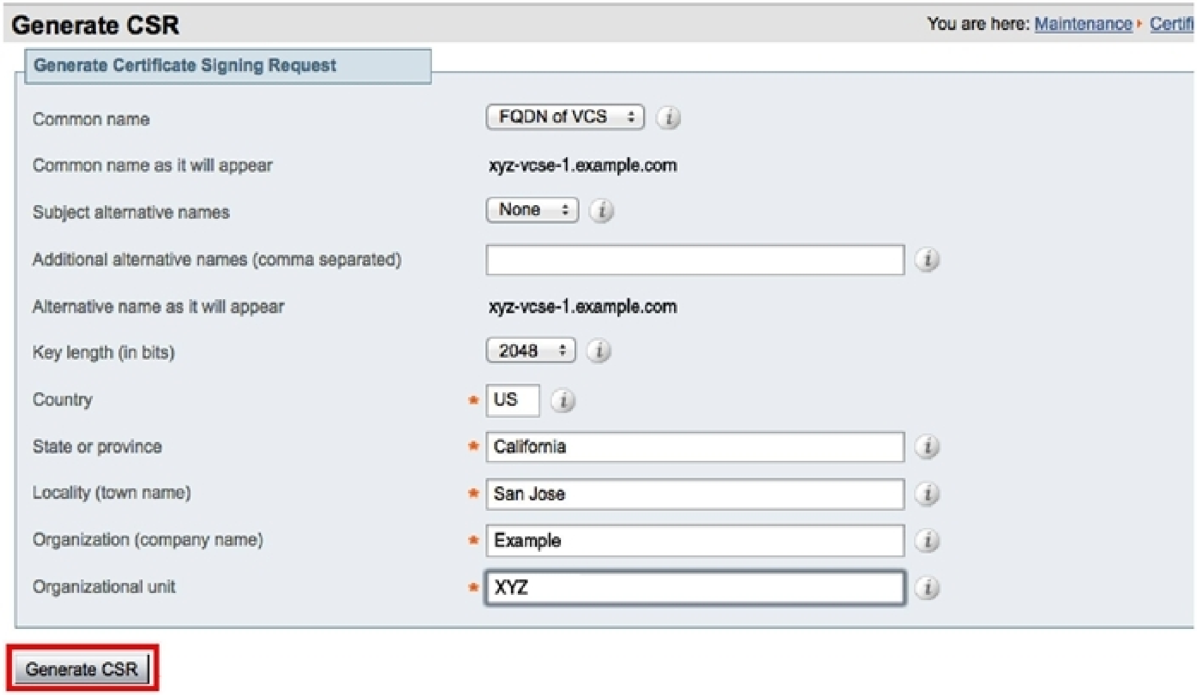
Certificate request: There is no certificate signing request in progress

Upload new certificate

Select the server private key file

Select the server certificate file

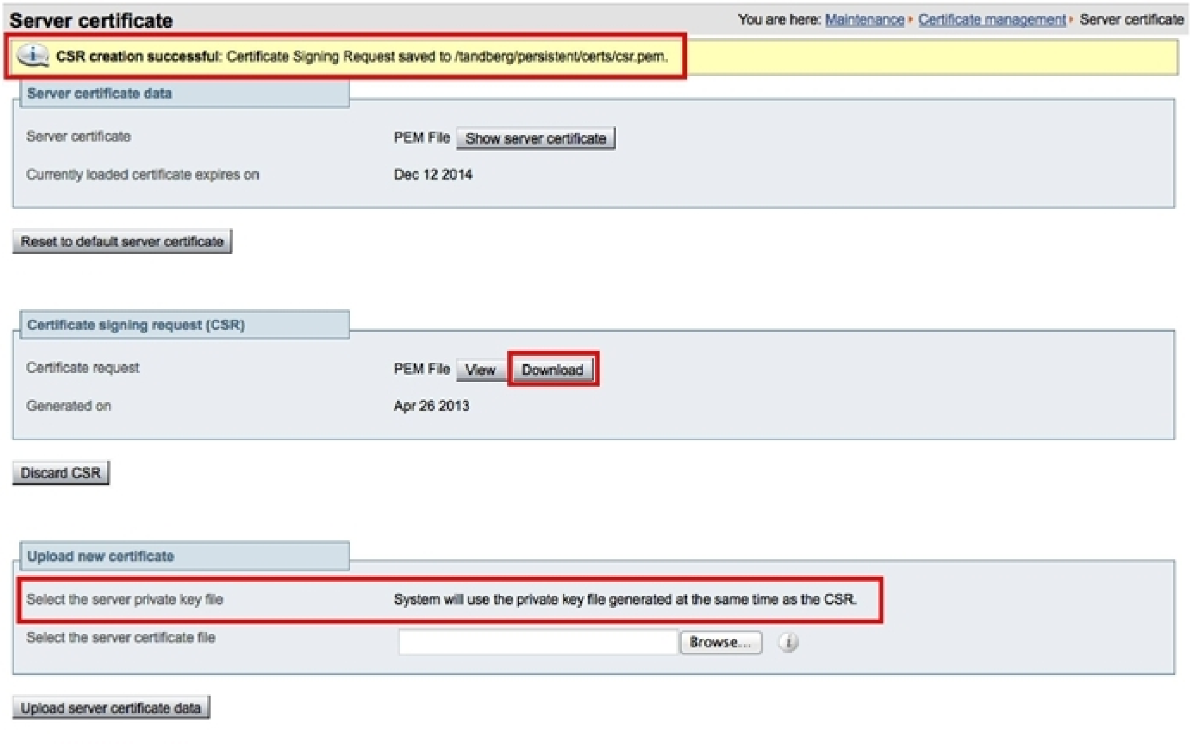
2. Enter the required information for the CSR and click **Generate CSR**.


Generate CSR
You are here: Maintenance ▸ Certifi
Generate Certificate Signing Request
Generate CSR

Common name	FQDN of VCS
Common name as it will appear	xyz-vcse-1.example.com
Subject alternative names	None
Additional alternative names (comma separated)	
Alternative name as it will appear	xyz-vcse-1.example.com
Key length (in bits)	2048
Country *	US
State or province *	California
Locality (town name) *	San Jose
Organization (company name) *	Example
Organizational unit *	XYZ

After clicking the Generate CSR button, the Server Certificate page is displayed along with a message indicating that CSR creation was successful.

Note: The private key is automatically generated as part of the CSR creation process. DO NOT click the option to Discard CSR, because this will force you to regenerate the CSR and will discard the previously generated private key.



Server certificate

You are here: Maintenance ▸ Certificate management ▸ Server certificate

CSR creation successful: Certificate Signing Request saved to /tandberg/persistent/certs/csr.pem.

Server certificate data

Server certificate: PEM File [Show server certificate]

Currently loaded certificate expires on: Dec 12 2014

[Reset to default server certificate]

Certificate signing request (CSR)

Certificate request: PEM File [View] [Download]

Generated on: Apr 26 2013

[Discard CSR]

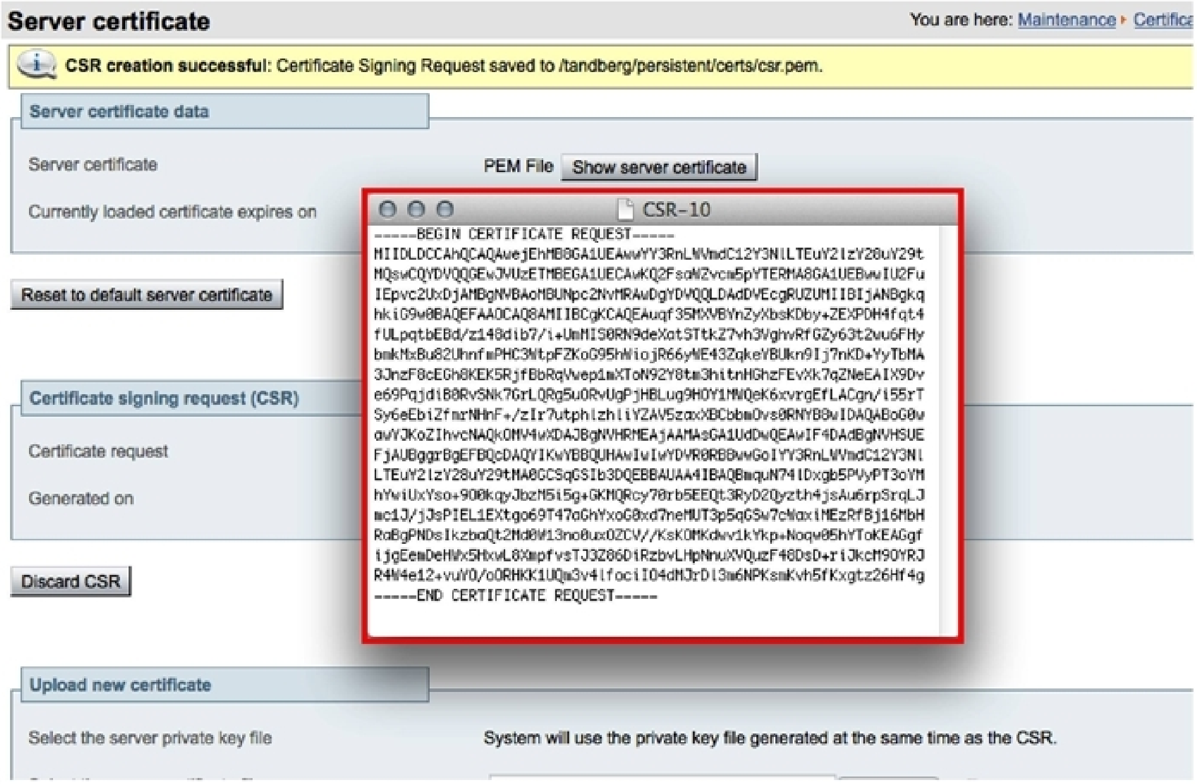
Upload new certificate

Select the server private key file: System will use the private key file generated at the same time as the CSR.

Select the server certificate file: [Browse...]

[Upload server certificate data]

3. In order to complete the CSR process and receive a signed certificate from a supported public certificate authority (CA), you must download the CSR by clicking **Download**.
   Most certificate authorities will require the CSR to be provided in a PKCS#10 request format (shown below).



Server certificate

You are here: Maintenance ▸ Certifica

CSR creation successful: Certificate Signing Request saved to /tandberg/persistent/certs/csr.pem.

Server certificate data

Server certificate: PEM File [Show server certificate]

Currently loaded certificate expires on

[Reset to default server certificate]

Certificate signing request (CSR)

Certificate request

Generated on

[Discard CSR]

Upload new certificate

Select the server private key file: System will use the private key file generated at the same time as the CSR.

CSR-10

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDLDCCAhQCAQAwejEhMB8GA1UEAwwYY3RnLWVmdC12Y3NlLTEuY2lzY28uY29t
MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwIU2Fu
IEpvc2UxDjAMBgNVBAoMBUNpc2NvMRAwDgYDVQQLDAdDVEcgRUZUMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuqf35MXVBYnZyXbsKDby+ZEXPDH4fqt4
fULpqtbEBd/z148dib7/i+UmMIS0RN9deXotSTtkZ7vh3VghvRfGZy63t2wu6FHy
bmkMxBu82UhnfmPHC3NtpFZKoG95hWiojR66yNE43ZqkeYBUkn9Ij7nKD+YyTbMA
3JnzF8cEGh8KEK5RjfBbRqVwep1mXToN92Y8tm3hitnHGhzFEvXk7qZNeEAIX9Dv
e69PqjdiB0RvSNk7GrLQRg5uORvUgPjHBLug9HOY1MWQeK6xvrgEfLACgn/i55rT
Sy6eEbiZfmrNHnF+/zIr7utphlzhliYZAV5zaxXBCbbm0vs0RNYB8wIDAQABoG0w
awYJKoZIhvcNAQkOMV4wXDAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF4DAdBgNVHSUE
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwIwYDVR0RBBwwGoIYY3RnLWVmdC12Y3Nl
LTEuY2lzY28uY29tMA0GCSqGSIb3DQEBBQUAA4IBAQBmquN74lDxgb5PVyPT3oYM
hYwiUxYso+900kqyJbzM5i5g+GKMQRcy70rb5EEQt3RyD2Qyzth4jsAu6rpSrqLJ
mc1J/jJsPIEL1EXtgo69T47aGhYxoG0xd7neMUT3p5qGSw7cWaxiMEzRfBj16MbH
RaBgPNDsIkzbaQt2Md0W13no0uxOZCV//KsKOMKdwv1kYkp+Noqw05hYToKEAGgf
ijgEemDeHWx5HxwL8XmpfvsTJ3Z86DiRzbvLHpNnuXVQuzF48DsD+riJkcM9OYRJ
R4W4e12+vuY0/oORHKK1UQm3v4lfociI04dMJrDl3m6NPKsmKvh5fKxgtz26Hf4g
-----END CERTIFICATE REQUEST-----
```

4. Submit the CSR to your public CA.

   Note: Important: Make sure your public CA provides you with an SSL server certificate that includes both Server and Client Auth keys.

   Once you receive the SSL server certificate from your public CA, you are ready to install it on the Cisco Expressway-E or Cisco VCS Expressway

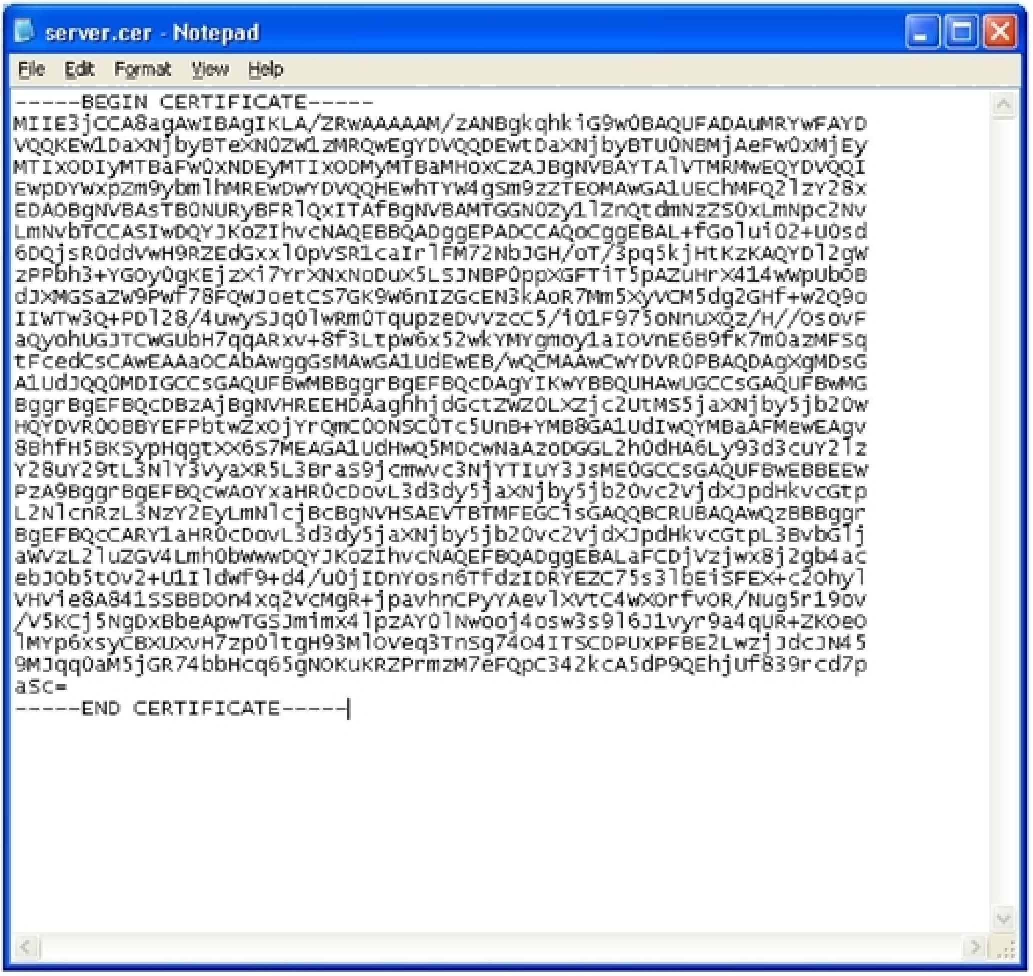
Installing the SSL Server Certificate on the Cisco Expressway-E or Cisco VCS Expressway

Note: Before installing the server certificate on the Cisco Expressway-E or Cisco VCS Expressway, make sure it is in the .PEM format. If the certificate you received is in a .CER format, you can convert it to a .PEM file by simply changing the file extension to .PEM.

CAUTION: The server certificate must not be stacked along with the root or intermediate CA Certificates.

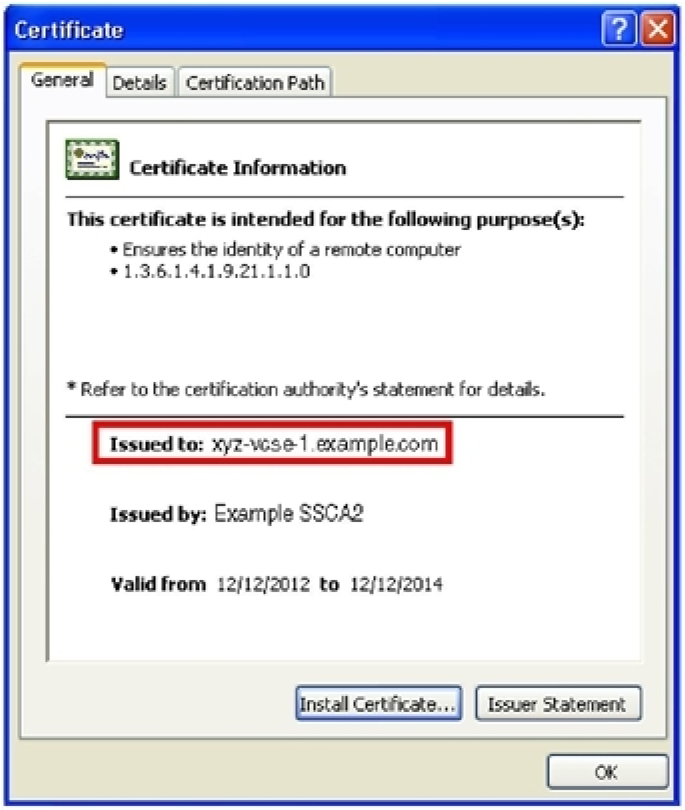
To install the SSL server certificate on the Cisco Expressway-E or Cisco VCS Expressway, do the following:

1. (Recommended) Open the server certificate in a text editing application such as Notepad and verify that you see a single certificate (noted by Begin and End Certificate brackets).



```
-----BEGIN CERTIFICATE-----
MIIE3jCCA8agAwIBAgIKLA/ZRwAAAAAM/zANBgkqhkiG9w0BAQUFADAuMRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDaXNjbyBTU0NBMjAeFw0xMjEy
MTIxODIyMTBaFw0xNDEyMTIxODMyMTBaMHoxCzAJBgNVBAYTAlVTMRMwEQYDVQQI
EwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEOMAwGA1UEChMFQ2lzY28x
EDAOBgNVBAsTB0NURyBFRlQxITAfBgNVBAMTGGN0Zy1lZnQtdmNzZS0xLmNpc2Nv
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+fGolui02+U0sd
6DQjsR0ddVwH9RZEdGxxl0pVSR1caIrlFM72NbJGH/oT/3pq5kjHtKzKAQYDl2gW
zPPbh3+YGOy0gKEjzXi7YrXNxNoDuX5LSJNBP0ppXGFTiT5pAZuHrX414wWpUbOB
dJXMGSaZw9Pwf78FQWJoetCS7GK9w6nIZGcEN3kAoR7Mm5XyVCM5dg2GHf+w2Q9o
IIWTw3Q+PDl28/4uwySJq0lwRm0TqupzeDvVzcC5/i01F975oNnuXQz/H//OsOvF
aQyohUGJTCWGUbH7qqARxv+8f3Ltpw6x52wkYMYgmoy1aIOvnE6B9fK7m0azMFSq
tFcedCsCAwEAAaOCAbAwggGsMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgXgMDsG
A1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwUGCCsGAQUFBwMG
BggrBgEFBQcDBzAjBgNVHREEHDAaghhjdGctZWZ0LXZjc2UtMS5jaXNjby5jb20w
HQYDVR0OBBYEFPbtwZxOjYrQmC0ONSC0Tc5UnB+YMB8GA1UdIwQYMBaAFMewEAgv
8BhfH5BKSypHqgtXX6S7MEAGA1UdHwQ5MDcwNaAzoDGGL2h0dHA6Ly93d3cuY2lz
Y28uY29tL3NlY3VyaXR5L3Bras9jcmwvc3NjYTIuY3JsME0GCCsGAQUFBwEBBEEw
PzA9BggrBgEFBQcwAoYxaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L2NlcnRzL3NzY2EyLmNlcjBcBgNVHSAEVTBTMFEGCisGAQQBCRUBAQAwQzBBBggr
BgEFBQcCARY1aHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL3BvbGlj
aWVzL2luZGV4Lmh0bWwwDQYJKoZIhvcNAQEFBQADggEBALaFCDjVzjwx8j2gb4ac
ebJOb5tOv2+U1IldwF9+d4/u0jIDnYosn6TfdzIDRYEZC75s3lbEiSFEX+c2Ohyl
VHVie8A841SSBBDOn4xq2VcMgR+jpavhnCPyYAevlXVtC4wXOrfVOR/Nug5r19ov
/V5KCj5NgDxBbeApwTGSJmimx4lpzAY0lNwOoj4osw3s9l6J1vyr9a4qUR+ZKOeO
lMYp6xsyCBXUXvH7zp0ltgH93MlOveq3TnSg74O4ITSCDPUxPFBE2LwzjJdcJN45
9MJqq0aM5jGR74bbHcq65gNOKuKRZPrmzM7eFQpC342kcA5dP9QEhjUf839rcd7p
aSc=
-----END CERTIFICATE-----
```

You may also want to verify that the validity of the server certificate by opening it as a .CER file. Here you should observe that the **Issued to** field is that of the Cisco Expressway-E or Cisco VCS Expressway server.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 1.3.6.1.4.1.9.21.1.1.0

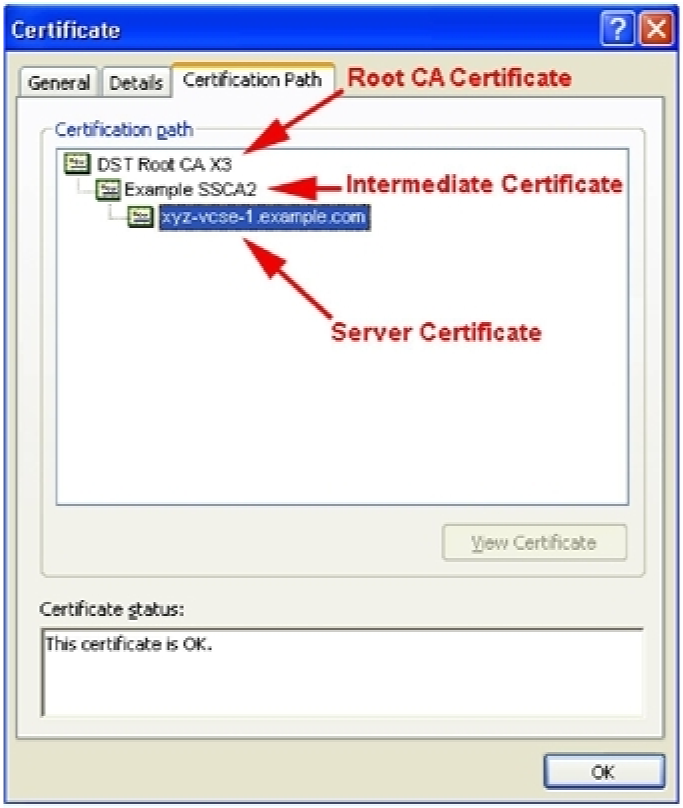
* Refer to the certification authority's statement for details.

Issued to: xyz-vcse-1.example.com

Issued by: Example SSCA2

Valid from 12/12/2012 to 12/12/2014

Tip: It is worth noting whether the CA that issued the certificate uses an intermediate CA or issues/signs certificates from a root CA. If an intermediate CA is involved then you'll need to "stack" or add the Intermediate CA Certificate to the Trusted CA Certificate.



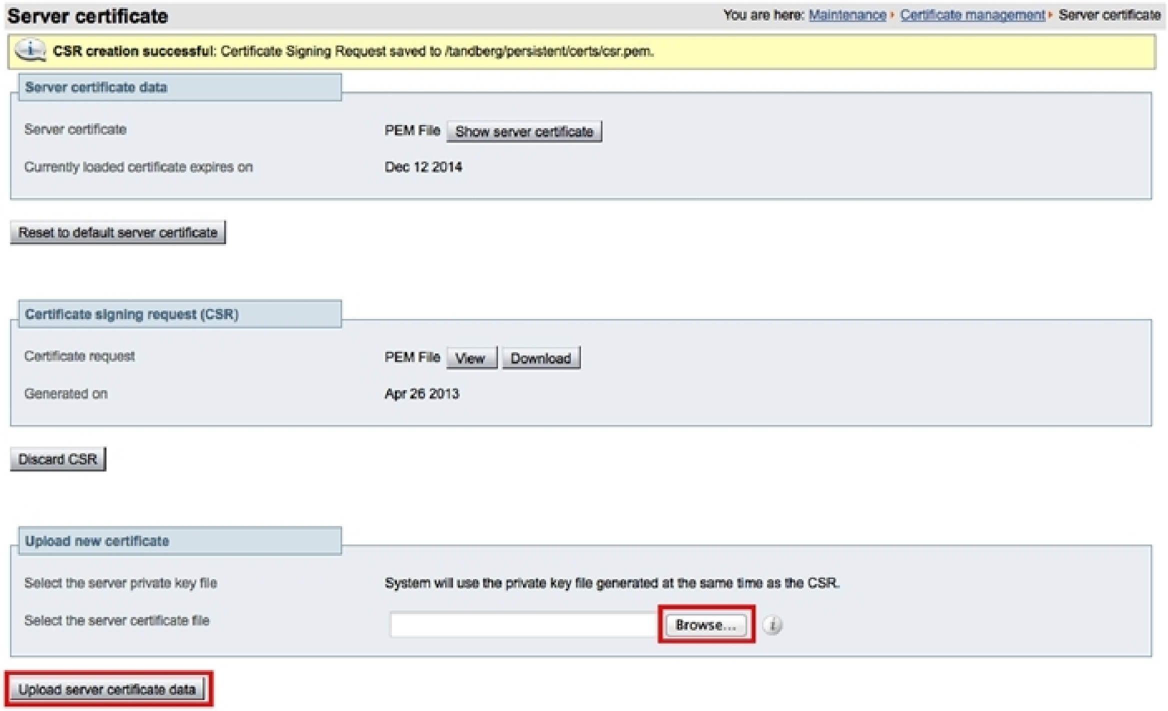
Certificate status:

This certificate is OK.

2. In Cisco Expressway-E or Cisco VCS Expressway:
   - X8.1, go to **Maintenance > Security certificates > Server certificate**.
   - X7.2.3, go to **Maintenance > Certificate management > Server certificate**.
3. Click **Browse** and select the server certificate that you received from the public CA and click **Open**.

   Note: The server certificate must be loaded on to the Expressway in the .PEM certificate format.

4. Click **Upload server certificate data**.



Server certificate

You are here: Maintenance ▸ Certificate management ▸ Server certificate

CSR creation successful: Certificate Signing Request saved to /tandberg/persistent/certs/csr.pem.

Server certificate data

Server certificate	PEM File
Currently loaded certificate expires on	Dec 12 2014

Certificate signing request (CSR)

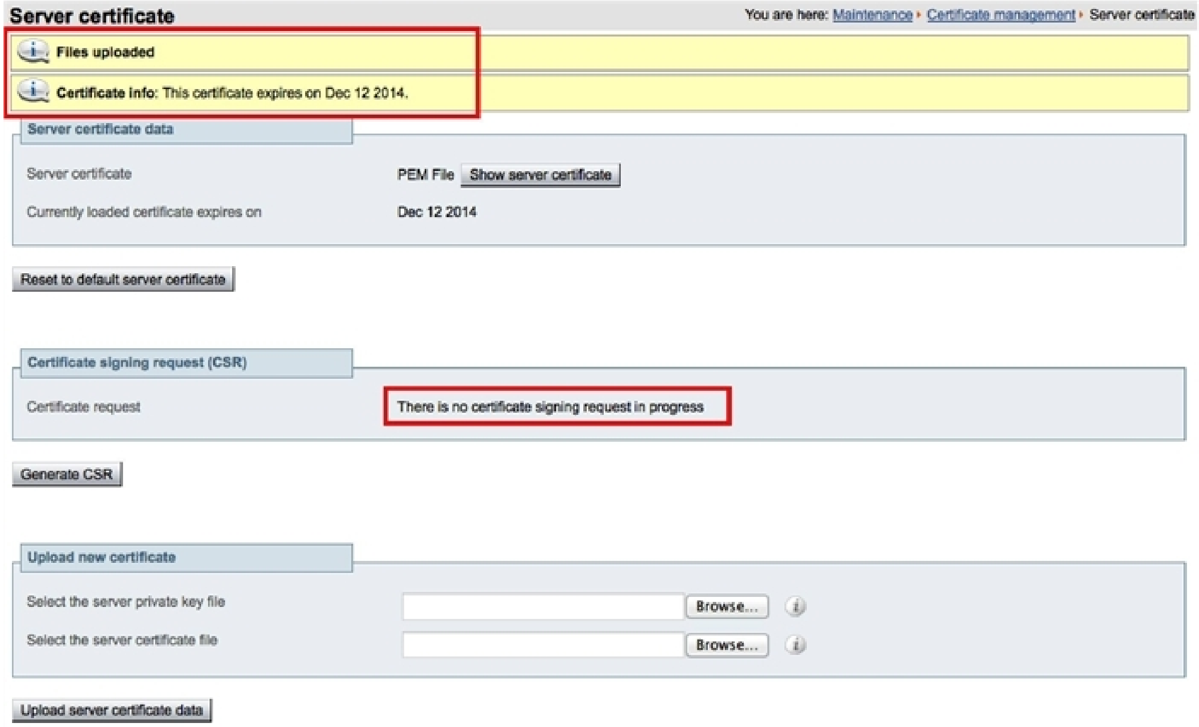
Certificate request	PEM File
Generated on	Apr 26 2013

Upload new certificate

Select the server private key file	System will use the private key file generated at the same time as the CSR.
Select the server certificate file	

Show server certificate
Reset to default server certificate
View
Download
Discard CSR
Browse...
Upload server certificate data

After uploading the server certificate, you'll see a message at the top of the page indicating that files were uploaded.



Server certificate

You are here: Maintenance ▸ Certificate management ▸ Server certificate

Files uploaded

Certificate info: This certificate expires on Dec 12 2014.

Server certificate data

Server certificate	PEM File
Currently loaded certificate expires on	Dec 12 2014

Certificate signing request (CSR)

Certificate request	There is no certificate signing request in progress

Upload new certificate

Select the server private key file	
Select the server certificate file	

Show server certificate
Reset to default server certificate
Generate CSR
Browse...
Browse...
Upload server certificate data

Configuring the Trusted CA Certificate List on the Cisco Expressway-E Cisco VCS Expressway

The version of Cisco VCS Expressway or Cisco Expressway-E that you are using will determine how you configure the trusted CA certificate list.

Cisco VCS Expressway X7.2.3

The default trusted CA certificate list for Cisco VCS Expressway X7.2.3 contains 140 certificates. It is very likely the public root CA that issued your server certificate is already part of the default trusted CA certificate list.

For details on how to configure the trusted CA certificate list on Cisco VCS Expressway X7.2.3, go to Configuring the Trusted CA Certificate List on Cisco VCS Expressway X7.2.3 [p.80].

Cisco VCS Expressway Upgraded from X7.2.3 to X8.1

If you upgraded your Cisco VCS Expressway from X7.2.3 to X8.1, the trusted CA certificate list from X7.2.3 will be retained.

For details on how to configure the trusted CA certificate list on Cisco VCS Expressway upgraded from X7.2.3 to X8.1, go to Configuring the Trusted CA Certificate List on Cisco VCS Expressway Upgraded from X7.2.3 to X8.1 [p.87]Configuring the Trusted CA Certificate List on Cisco VCS Expressway Upgraded from X7.2.3 to X8.1 [p.87]Configuring the Trusted CA Certificate List on Cisco VCS Expressway Upgraded from X7.2.3 to X8.1 [p.87]

Cisco Expressway-E or Cisco VCS Expressway X8.1

If you are using a freshly installed Cisco Expressway-E or Cisco VCS Expressway X8.1, you will need to load your own list of trusted CA certificates, because it does not (by default) contain any certificates in its default trusted CA certificate list.

In addition, you will need to add the root certificate used by the WebEx cloud to the default trusted CA certificate list on your Cisco Expressway-E or Cisco VCS Expressway X8.1, which is DST Root CA X3.

For details on how to configure the trusted CA certificate list on a freshly installed Cisco Expressway-E or Cisco VCS Expressway X8.1, go to Configuring the Trusted CA Certificate List on Cisco Expressway-E or Cisco VCS Expressway X8.1 or Later [p.92]Configuring the Trusted CA Certificate List on Cisco Expressway-E or Cisco VCS Expressway X8.1 or Later [p.92]Configuring the Trusted CA Certificate List on Cisco Expressway-E or Cisco VCS Expressway X8.1 or Later [p.92] .

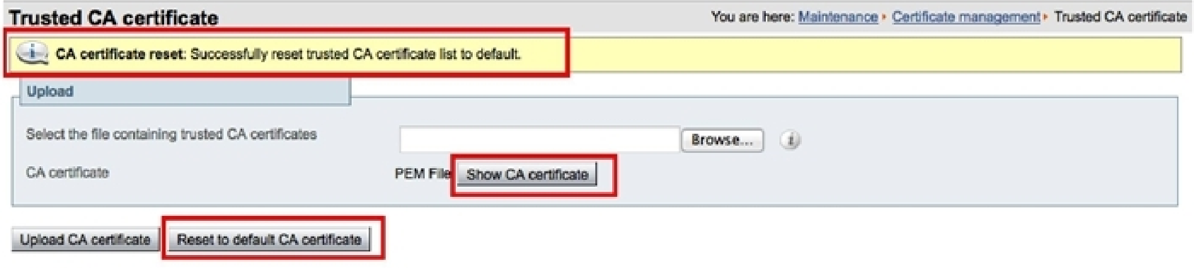
Configuring the Trusted CA Certificate List on Cisco VCS Expressway X7.2.3

If the default trusted CA certificate list is not currently in use, we recommend that you reset it back to the default CA Certificate. This simplifies the process of ensuring that the required certificates are in place.

Resetting the Trusted CA Certificate List on Cisco VCS Expressway X7.2.3

To reset the trusted CA certificate list on the Cisco VCS Expressway X7.2.3, do the following:

1. Go to **Maintenance > Certificate management > Trusted CA certificate** and click **Reset to default CA Certificate**.



Trusted CA certificate

You are here: Maintenance ▸ Certificate management ▸ Trusted CA certificate

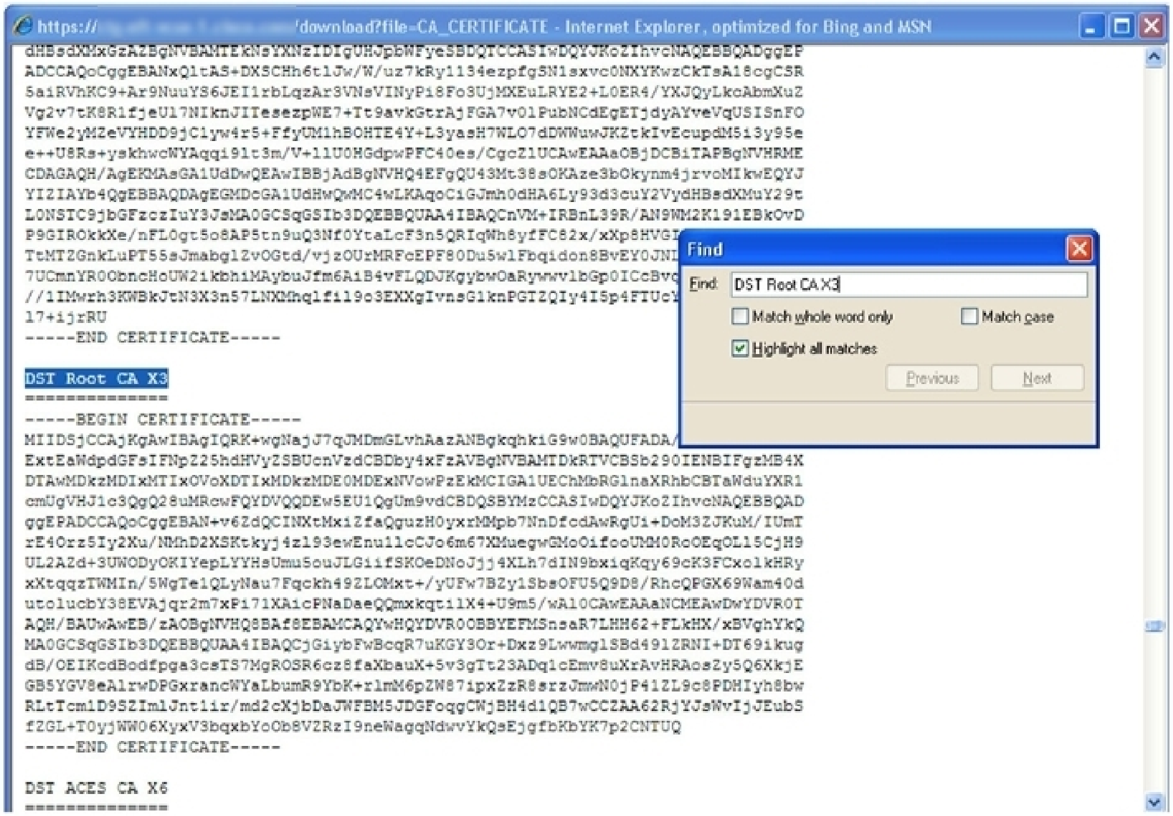
CA certificate reset: Successfully reset trusted CA certificate list to default.

Upload
Select the file containing trusted CA certificates
Browse...
CA certificate
PEM File
Show CA certificate
Upload CA certificate
Reset to default CA certificate

Note: Your Cisco VCS Expressway must trust the certificate issuer of the server certificate that is passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud.

If the server certificate was issued by the root CA (rather than an intermediate CA), it is likely that the root certificate is part of the default trusted CA list.

2. It is best practice to verify that the proper root certificate is present. You may do this by clicking **Show CA certificate.**
This will open in a new window displaying the default Trusted CA list that is currently loaded on the Cisco VCS Expressway.
3. Search for the root CA that issued the server certificate.



https://[redacted]/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN

```
dHBsdXMxGzAZBgNVBAMTEkNsYXNzIDIgUHJpbWFyeSBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANxQltAS+DX5CHh6tlJw/W/uz7kRy1134ezpfg5N1sxvc0NXYKwzCkTsA18cgC5R
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsVINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeUl7NIknJITesezpWE7+Tt9avkGtrAjFGA7v0lPubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWWuwJKZtkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqqi9lt3m/V+llU0HGdpwPFC40es/CgcZlUCAwEAAaOBjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvoMIkwEQYJ
YIZIAYb4QgEBBAQDAgEGMDcGA1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly93d3cuY2VydHBsdXMuY29t
L0NSTC9jbGFzczIuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkkXe/nFL0gt5o8AP5tn9uQ3Nf0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVGI
TtMTZGnkLuPT55sJmabglZvOGtd/vjzOUrMRFcEPF80Du5wlFbqidon8BvEY0JNI
7UCmnYR0ObncHoUW2ikbhiMAybuJfm6AiB4vFLQDJKgybwOaRywwvlbGp0ICcBvq
//1IMwrh3KWBkJtN3X3n57LNXMhqlfil9o3EXXgIvnsG1knPGTZQIy4I5p4FTUcY
17+ijrRU
-----END CERTIFICATE-----

DST Root CA X3
==============
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVowPzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQQDEw5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEqOLl5CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRy
xXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjE
GB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubS
fZGL+T0yjWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
==============
```

If the server certificate is issued by the top level root CA and NOT by an intermediate CA and the valid root CA certificate is present in the default trusted CA certificate list, then certificate configuration on the Cisco VCS Expressway is complete.
If the server certificate is issued by an intermediate CA, go to the next section.

Note: If the server certificate for the top-level root CA that issued your server certificate is not part of the trusted CA certificate list, you must add it using the same procedure that is described for stacking the intermediate certificate, detailed in the next section.

Cisco VCS Expressway will need to trust the certificate issuer of the server certificate that is passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud.

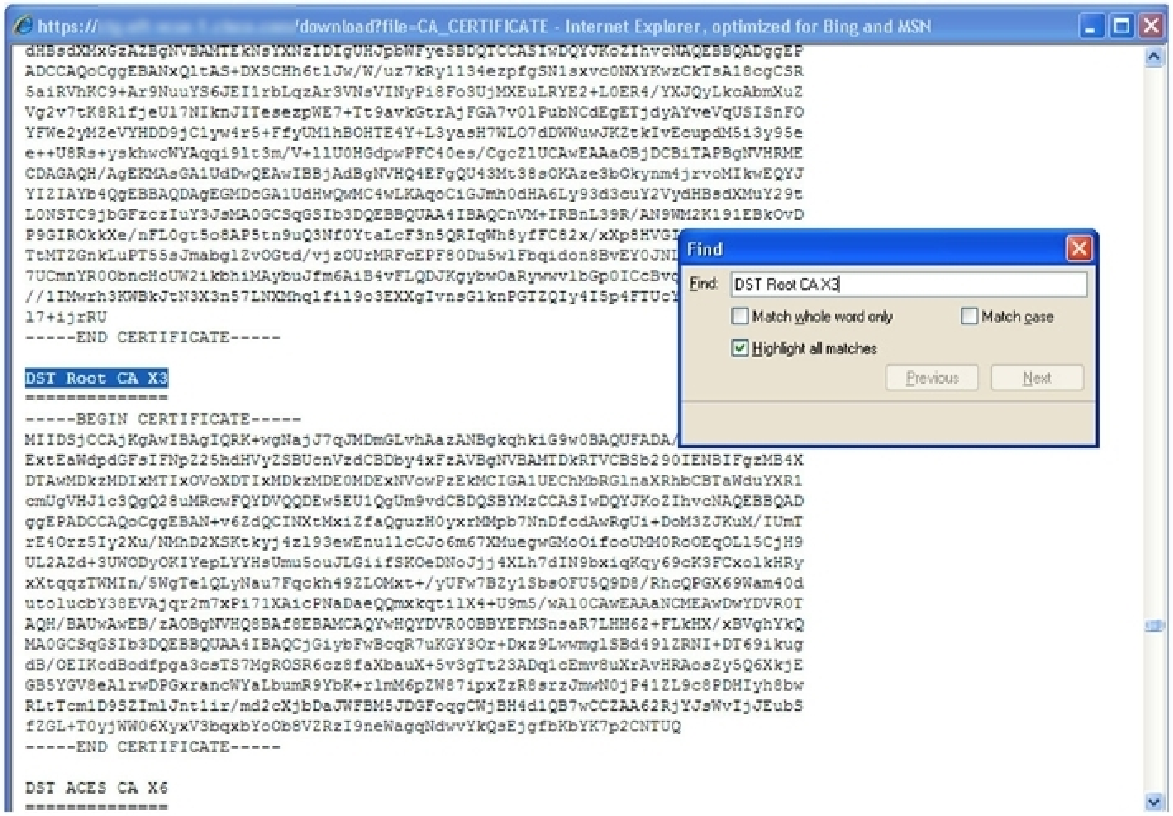
The Default Trusted CA List on the Cisco VCS Expressway has already the public root CA Certificate for the server certificate the cloud will present. The root CA for the WebEx cloud is DST Root CA X3 with an intermediate CA of Cisco SSCA2.

If the server certificate was issued by the root CA (rather than an intermediate CA), it is likely that the root certificate is part of the default trusted CA list.

It is best practice to verify that the proper root certificate is present. You may do this by clicking **Show CA certificate.**

This will open in a new window displaying the default Trusted CA list that is currently loaded on the Cisco VCS Expressway.

Search for the root CA that issued the server certificate.


https://[redacted]'download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN
Find
Find DST Root CA X3
□ Match whole word only
□ Match case
☑ Highlight all matches
Previous
Next

```
dHBsdXMxGzAZBgNVBAMTEkNsYXNzIDIgUHJpbWFyeSBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANxQltAS+DXSCHh6tlJw/W/uz7kRy1134ezpfgSN1sxvc0NXYKwzCkTsA18cgCSR
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsVINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeUl7NIknJITesezpWE7+Tt9avkGtrAjFGA7v0lPubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWWuwJKZtkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqqi9lt3m/V+llU0HGdpwPFC40es/CgcZlUCAwEAAaOBjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvoMIkwEQYJ
YIZIAYb4QgEBBAQDAgEGMDcGA1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly93d3cuY2VydHBsdXMuY29t
L0NSTC9jbGFzczIuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkkXe/nFL0gt5o8AP5tn9uQ3Nf0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVGI
TtMTZGnkLuPT55sJmabglZvOGtd/vjzOUrMRFcEPF80Du5wlFbqidon8BvEY0JNI
7UCmnYR0ObncHoUW2ikbhiMAybuJfm6AiB4vFLQDJKgybwOaRywwvlbGp0ICcBvq
//1IMwrh3KWBkJtN3X3n57LNXMhqlfil9o3EXXgIvnsG1knPGTZQIy4I5p4FTUcY
l7+ijrRU
-----END CERTIFICATE-----

DST Root CA X3
==============
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVowPzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQQDEw5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEqOLl5CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRy
xXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjE
GB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubS
fZGL+T0yjWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
==============
```

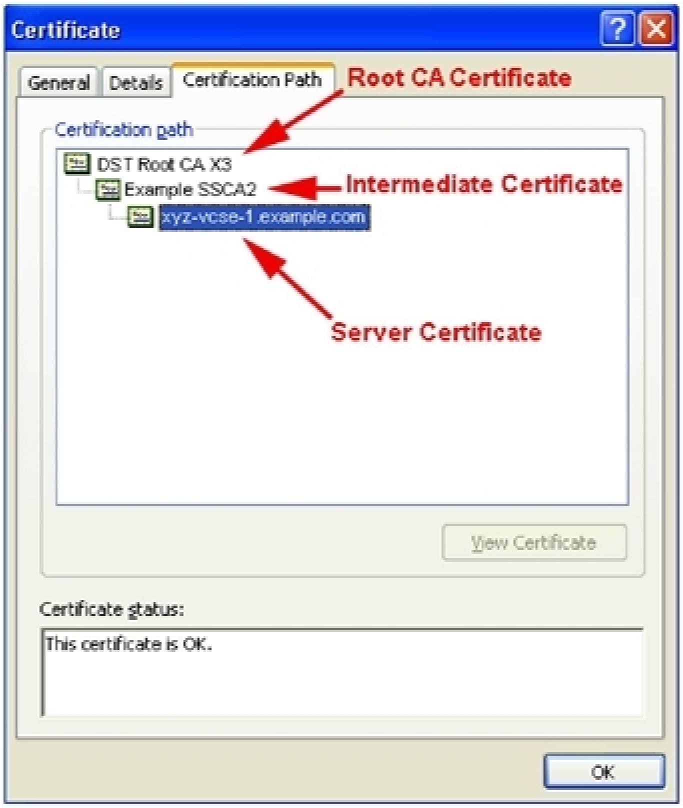
If the server certificate is issued by the top level root CA and NOT by an intermediate CA and the valid root CA certificate is present in the default Trusted CA list, then certification configuration on the Cisco VCS Expressway is complete. If the server certificate is issued by an intermediate CA, go to the next section.

Stacking the Intermediate Certificate CA Certificate in the Trusted CA Certificate List on Cisco VCS Expressway X7.2.3

In some cases, root CAs will use an intermediate CA to issue certificates.

If the server certificate is issued by an intermediate CA, then you will need to add the intermediate CA certificate to the default Trusted CA list.

Figure 16: Server Certificate in .CER File Format

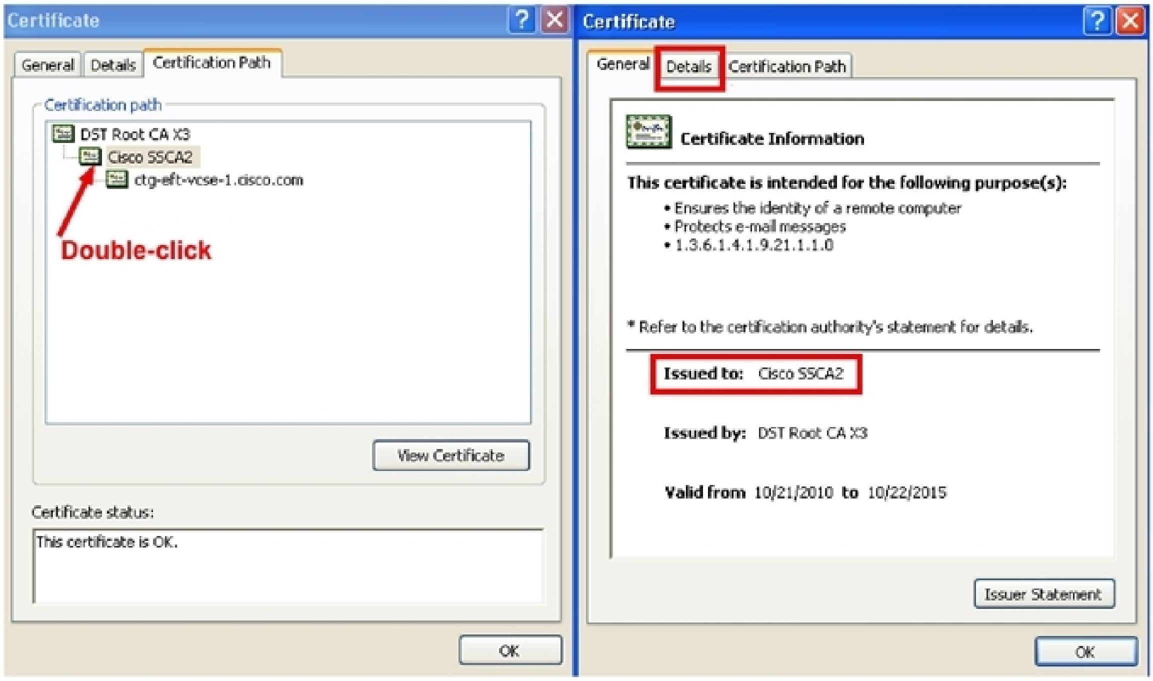


This certificate is OK.

Unless the public CA provided you the exact intermediate and root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure you that you are stacking the correct intermediate CA certificate.

1. Open the server certificate as a .CER file (see Figure 16: Server Certificate in .CER File Format [p.83]).
2. Click the **Certification Path** tab, then double-click the **Intermediate Certificate**.
   This opens the intermediate CA certificate in a separate certificate viewer.
3. Make sure the **Issued to** field displays the name of the Intermediate CA.

4. Click the **Details** tab followed by **Copy to File…**



This certificate is OK.

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Protects e-mail messages
- 1.3.6.1.4.1.9.21.1.1.0

* Refer to the certification authority's statement for details.

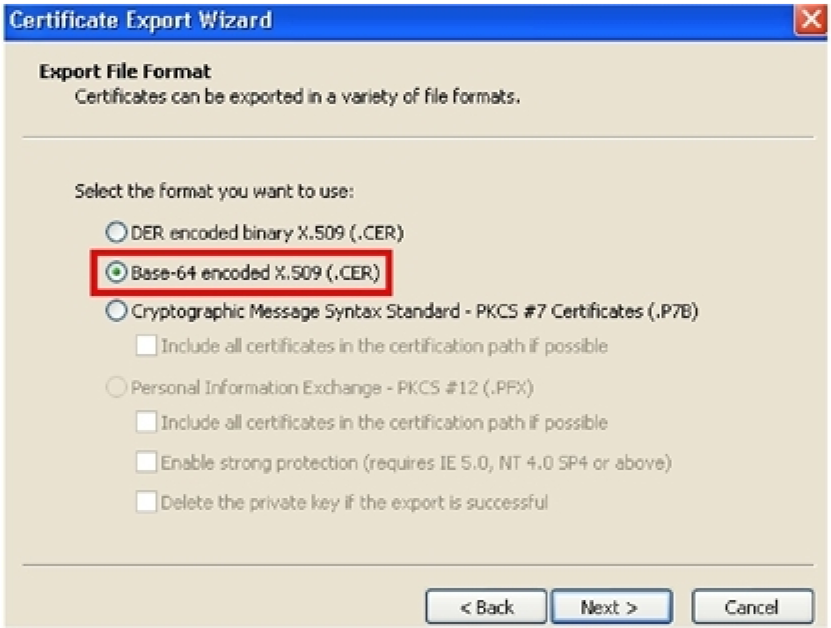
Issued to: Cisco SSCA2

Issued by: DST Root CA X3

Valid from 10/21/2010 to 10/22/2015

The **Welcome to the Certificate Export Wizard** appears.

5. Click **Next**.
6. Choose *Base-64 encoded X.509 (.CER)* as the Export File Format and click **Next**.

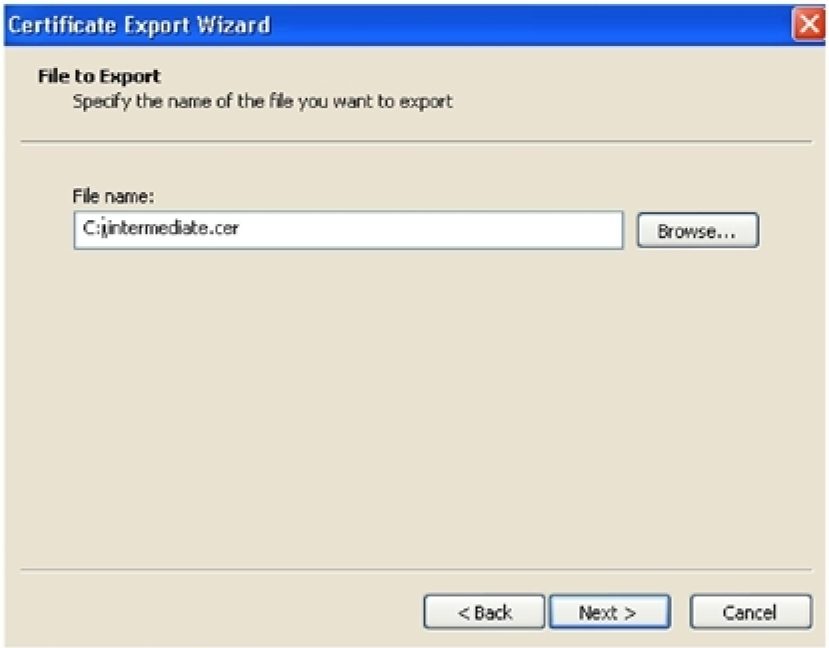


Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful

7. Name the file, click **Next**, and then click **Finish**.

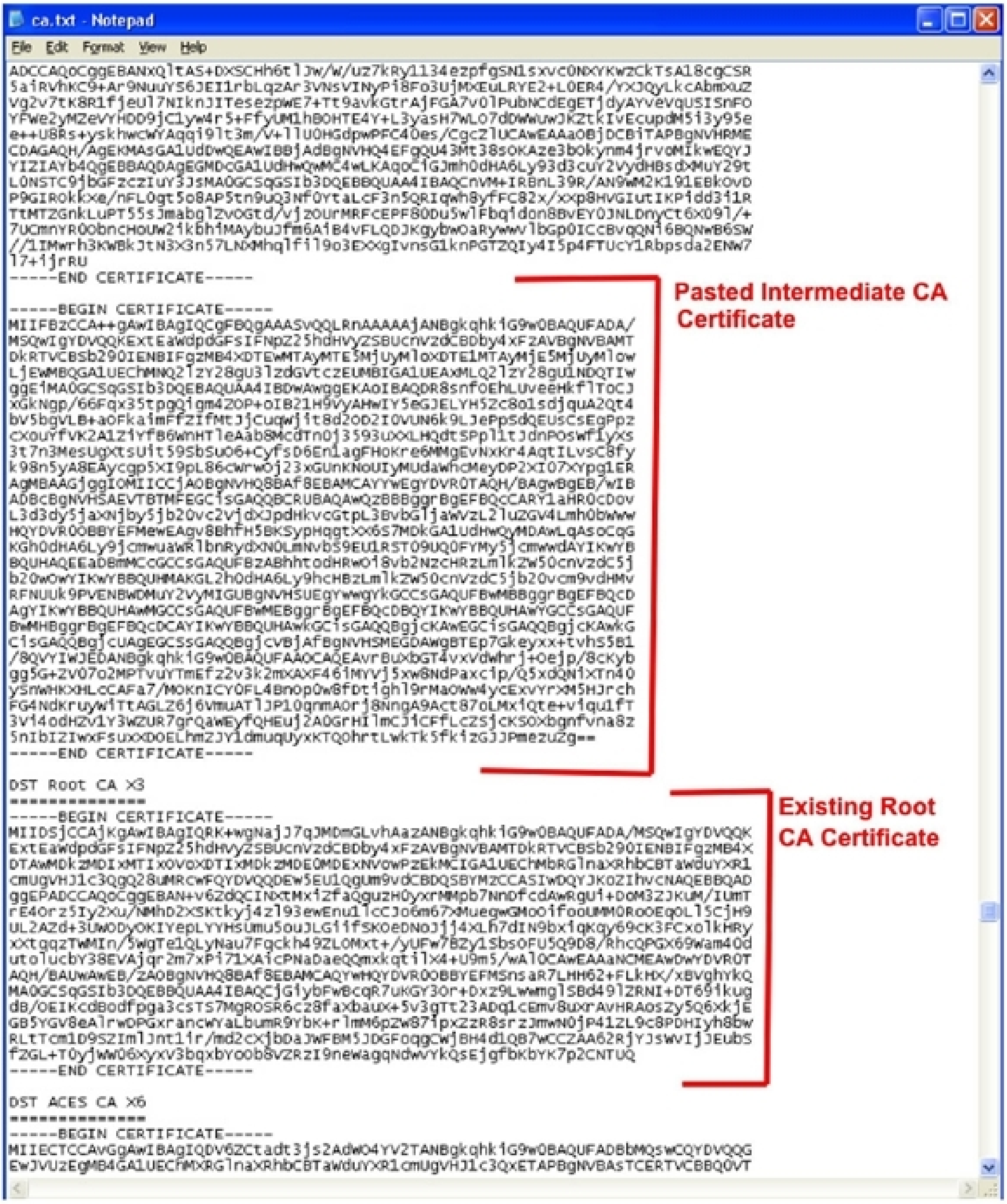


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
Browse...
< Back
Next >
Cancel

File name: C:\intermediate.cer

8. Copy the default Trusted CA list from the Cisco VCS Expressway by going to **Maintenance > Certificate management > Trusted CA certificate** and clicking **Show CA Certificate**. In the window that opens, select all contents.
9. Paste the contents into a text editing application such as Notepad.
10. Open the intermediate.cer file within a new window of your text editing application and copy the contents to your clipboard.
11. Do a search for the existing root CA certificate within the text file that contains the contents of the default Trusted CA list.
12. Paste the intermediate CA certificate above the root certificate.

13. Save the text file as .PEM file (Example: **`NewDefaultCA.pem`**)

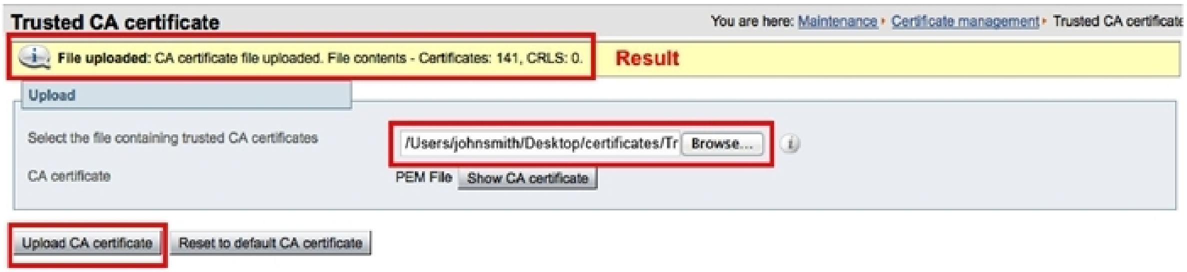

ca.txt - Notepad
File Edit Format View Help
Pasted Intermediate CA Certificate
Existing Root CA Certificate

```
ADCCAQoCggEBANxQ1tAS+DxSCHh6t1Jw/W/uz7kRy1134ezpfgSN1sxvc0NXYKwzCkTsA18cgCSR
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsVINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeUl7NIknJITesezpWE7+Tt9avkGtrAjFGA7v0lPubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWwuwJKZtkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqqi9lt3m/V+llU0HGdpwPFC40es/CgcZ1UCAwEAAaOBjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvoMIkwEQYJ
YIZIAYb4QgEBBAQDAgEGMDcGA1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly93d3cuY2VydHBsdXMuY29t
L0NSTC9jbGFzczIuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkkXe/nFL0gt5o8AP5tn9uQ3Nf0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVGIutIKPidd3i1R
TtMTZGnkLuPT55sJmabglZvOGtd/vjzOUrMRFcEPF80Du5wlFbqidon8BvEY0JNLDnyCt6X09l/+
7UCmnYR0ObncHoUW2ikbhiMAybuJfm6AiB4vFLQDJKgybwOaRywwvlbGp0ICcBvqQNi6BQNwB6SW
//1IMwrh3KWBkJtN3X3n57LNXMhqlfil9o3EXXgIvnsG1knPGTZQIy4I5p4FTUcY1Rbpsda2ENW7
l7+ijrRU
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIFBzCCA++gAwIBAgIQCgFBQgAAASVQQLRnAAAAAjANBgkqhkiG9w0BAQUFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTEwMTAyMTE5MjUyMloXDTE1MTAyMjE5MjUyMlow
LjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEUMBIGA1UEAxMLQ2lzY28gU1NDQTIw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDR8snfOEhLUveeHkflToCJ
xGkNgp/66Fqx35tpgQigm4ZOP+oIB21H9VyAHwIY5eGJELYH52c8o1sdjquA2Qt4
bV5bgVLB+aOFkaimFfZIfMtJjCuqwjit8d2OD2I0VUN6k9LJePpSdQEUSCsEgPpz
cXOuYfVK2A1ZiYfB6WnHTleAab8McdTn0j3593uXXLHQdt5Ppl1tJdnPOswfIyxs
3t7n3MesUgXtsUit59SbSuO6+CyfsD6En1agFHoKre6MMgEvNxKr4AqtILvsC8fy
k98n5yA8EAycgp5XI9pL86cWrwOj23xGUnKNoUIyMUdawhcMeyDP2XI07XYpg1ER
AgMBAAGjggIOMIICCjAOBgNVHQ8BAf8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB/wIB
ADBcBgNVHSAEVTBTMFEGCisGAQQBCRUBAQAwQzBBBggrBgEFBQcCARY1aHR0cDov
L3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL3BvbGljaWVzL2luZGV4Lmh0bWww
HQYDVR0OBBYEFMewEAgv8BhfH5BKSypHqgtXX6S7MDkGA1UdHwQyMDAwLqAsoCqG
KGh0dHA6Ly9jcmwuaWRlbnRydXN0LmNvbS9EU1RST09UQ0FYMy5jcmwwdAYIKwYB
BQUHAQEEaDBmMCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcHRzLmlkZW50cnVzdC5j
b20wOwYIKwYBBQUHMAKGL2h0dHA6Ly9hcHBzLmlkZW50cnVzdC5jb20vcm9vdHMv
RFNUUk9PVENBWDMuY2VyMIGUBgNVHSUEgYwwgYkGCCsGAQUFBwMBBggrBgEFBQcD
AgYIKwYBBQUHAwMGCCsGAQUFBwMEBggrBgEFBQcDBQYIKwYBBQUHAwYGCCsGAQUF
BwMHBggrBgEFBQcDCAYIKwYBBQUHAwkGCisGAQQBgjcKAwEGCisGAQQBgjcKAwkG
CisGAQQBgjcUAgEGCSsGAQQBgjcVBjAfBgNVHSMEGDAWgBTEp7Gkeyxx+tvhS5B1
/8QVYIWJEDANBgkqhkiG9w0BAQUFAAOCAQEAvrBuXbGT4vxVdwhrj+Oejp/8cKyb
gg5G+2V07o2MPTvuYTmEfz2v3k2mXAXF46iMYVj5xw8NdPaxcip/Q5xdQN1XTn40
ySnWHKXHLoCAFa7/MOKnICY0FL4BnOp0w8fDtighl9rMaOWw4ycExvYrXM5HJrch
FG4NdkruywiTtAGLZ6j6VmuATlJP10gnmAOrj8NngA9Act87oLMxiQte+viqu1fT
3vi4odHZv1Y3WZUR7grQaWEyfQHEuj2AOGrHIlmCJiCFfLcZSjcKSOxbgnfvna8z
5nIbIZIwxFsuXXDOELhmZJY1dmuqUyxKTQOhrtLwkTk5fkizGJJPmezuZg==
-----END CERTIFICATE-----

DST Root CA X3
==============
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/MSQwIgYDVQQK
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVowPzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQQDEw5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEqOLl5CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRy
xXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjE
GB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubS
f2GL+T0yjWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
==============
-----BEGIN CERTIFICATE-----
MIIECTCCAvGgAwIBAgIQDV6ZCtadt3js2AdWO4YV2TANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQG
EwJVUzEgMB4GA1UEChMXRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QxETAPBgNVBAsTCERTVCBBQ0VT
```

Note: If the root CA is not part of the default trusted CA list, follow same procedure of stacking the intermediate CA certificate.

14. Click **Browse**, find your newly created/stacked Trusted CA list and click **Open**.

15. Click **Upload CA certificate**.



Trusted CA certificate

You are here: Maintenance ▸ Certificate management ▸ Trusted CA certificate

File uploaded: CA certificate file uploaded. File contents - Certificates: 141, CRLS: 0.

Result

Upload

Select the file containing trusted CA certificates: /Users/johnsmith/Desktop/certificates/Tr

CA certificate: PEM File

Certificate configuration on Cisco VCS Expressway X7.2.3 is complete.

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to *Certificate creation and use with Cisco VCS Deployment Guide* at the following location:

https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Certificate_Creation_and_Use_Deployment_Guide_X7-2.pdf

Configuring the Trusted CA Certificate List on Cisco VCS Expressway Upgraded from X7.2.3 to X8.1

If the default trusted CA certificate list is not currently in use, we recommend that you reset it back to the default CA Certificate. This simplifies the process of ensuring that the required certificates are in place.

- For details on how to reset the default trusted CA list, refer to the next section, Resetting the Trusted CA Certificate List on Cisco VCS Expressway Upgraded from X7.2.3

In addition, you must add the certificates used during the client/server SSL handshake with the WebEx cloud to the default trusted CA certificate list.

- For details on how to add the certificates used during the client/server SSL Handshake with the WebEx cloud, refer to the section Updating Certificates on Cisco Expressway-E or Cisco VCS Expressway

IMPORTANT: In the past, WebEx used a certificate that was issued under the Root CA ’DST Root CA X3’ to secure traffic between the customer premises and WebEx. We are revoking that certificate and replacing it with new certificates. Your VCS Expressway MUST trust the new root certificate authorities in order support the new WebEx certificates. If these certificates are not in your Trusted CA list, TelePresence calls may fail to join.

To complete the certificates configuration for a VCS Expressway upgraded from X7.2.3 to X8.1, you must add the CA certificate of the CA that issued your server certificate.

- For details on how to add the CA certificate for the CA that issued your server certificate, refer to: Adding the Root or Intermediate CA Certificate to VCS Expressway

Resetting the Trusted CA Certificate List on Cisco VCS Expressway Upgraded from X7.2.3 to X8.1

To reset the trusted CA certificate list on the Cisco VCS Expressway X8.1, do the following:

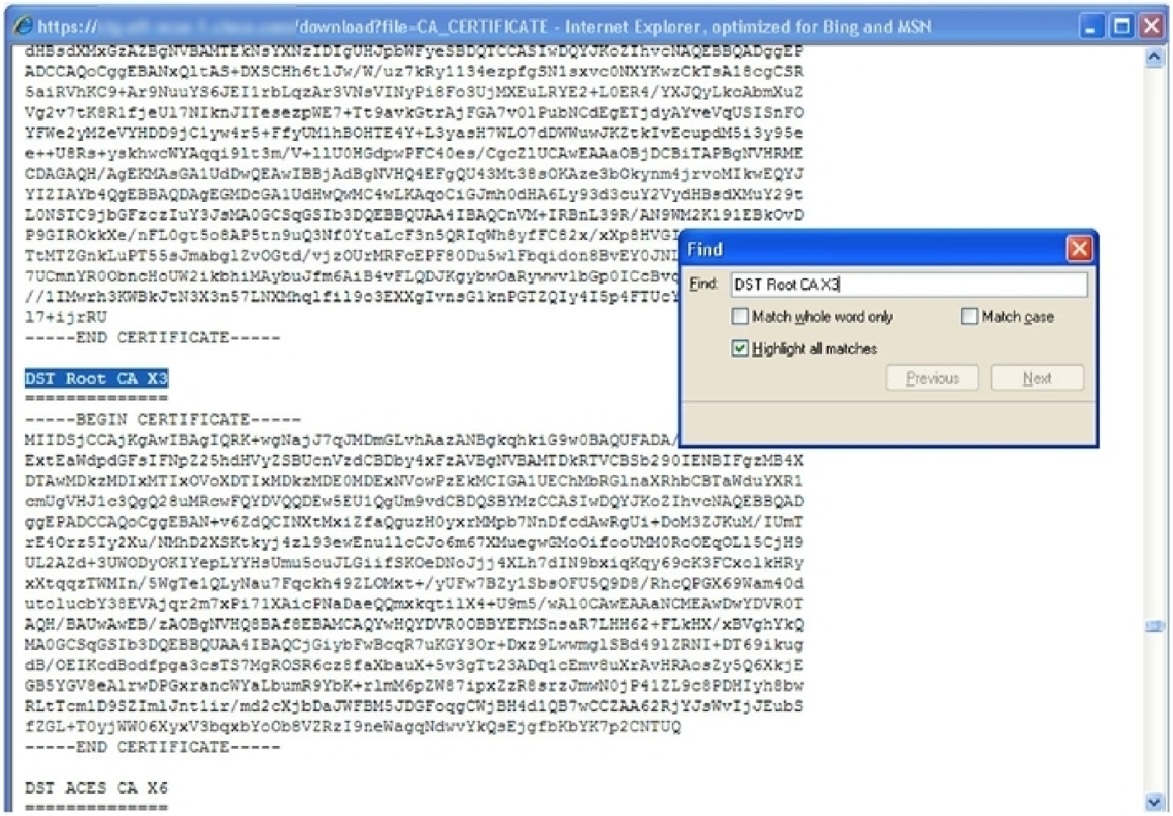
1. Go to **Maintenance > Security certificates > Trusted CA certificate** and click **Reset to default CA certificate**.

   Note: Your Cisco VCS Expressway must trust the certificate issuer of the server certificate that is passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud.

   If the server certificate was issued by the root CA (rather than an intermediate CA), it is likely that the root certificate is part of the default trusted CA list.

2. It is best practice to verify that the proper root certificate is present. You may do this by clicking **Show all (PEM file).**
   This will open in a new window displaying the default Trusted CA list that is currently loaded on the Cisco VCS Expressway.

3. Search for the root CA that issued the server certificate.



https://[redacted]/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN

```
dHBsdXMxGzAZBgNVBAMTEkNsYXNzIDIgUHJpbWFyeSBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANxQltAS+DXSCHh6tlJw/W/uz7kRy1134ezpfgSN1sxvc0NXYKwzCkTsA18cgCSR
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsVINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeUl7NIknJITesezpWE7+Tt9avkGtrAjFGA7v0lPubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWWuwJKZtkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqqi9lt3m/V+llU0HGdpwPFC40es/CgcZlUCAwEAAaOBjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvoMIkwEQYJ
YIZIAYb4QgEBBAQDAgEGMDcGA1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly93d3cuY2VydHBsdXMuY29t
L0NSTC9jbGFzczIuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkkXe/nFL0gt5o8AP5tn9uQ3Nf0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVGI
TtMTZGnkLuPT55sJmabglZvOGtd/vjzOUrMRFcEPF80Du5wlFbqidon8BvEY0JNI
7UCmnYR0ObncHoUW2ikbhiMAybuJfm6AiB4vFLQDJKgybwOaRywwvlbGp0ICcBvq
//1IMwrh3KWBkJtN3X3n57LNXMhqlfil9o3EXXgIvnsG1knPGTZQIy4I5p4FTUcY
l7+ijrRU
-----END CERTIFICATE-----

DST Root CA X3
==============
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVowPzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQQDEw5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEqOLl5CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRy
xXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjE
GB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubS
fZGL+T0yjWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
==============
```

Find

Find: DST Root CA X3

☐ Match whole word only ☐ Match case

☑ Highlight all matches

If the server certificate is issued by the top level root CA and NOT by an intermediate CA and the valid root CA certificate is present in the default trusted CA certificate list, then certificate configuration on the Cisco VCS Expressway is complete.

If the server certificate is issued by an intermediate CA or if the certificate for the top-level root CA that issued your server certificate is not part of the trusted certificate list, you must add it to the list, as detailed in the next section.

Updating Certificates on Cisco Expressway-E or Cisco VCS Expressway X8.1

Your Cisco Expressway-E or Cisco VCS Expressway must trust the certificate issuer of the server certificates that are passed by the server during the client/server SSL Handshake with the WebEx cloud. In order to do this, you must add these certificates to the trusted CA list on your Cisco Expressway-E or Cisco VCS Expressway.
To add these certificates to the trusted CA certificate list, do the following:

a. Go to each of the following links, copy and paste the contents of the displayed certificate into individual text files and save each with the file extension of .PEM:
   i. VeriSign Class 3 Public Primary CA
   ii. VeriSign Class 3 Primary CA - G5
   iii. VeriSign Class 3 Public Primary CA - G3
   iv. QuoVadis Root CA 2

   For example, the first one would be:
   `Class-3-Public-Primary-Certification-Authority.pem`

   Note: If you are NOT using Certificate Revocation or do NOT have a Certificate Revocation policy active on your VCS-Expressway or Expressway-E device, skip to step 3.

b. If you are using ‘automatic’ certificate revocation, temporarily disable it:
   i. On the VCS/Expressway, go to: **Maintenance >Security certificates > CRL Management**
   ii. Set automatic CRL updates to *disabled*

   Note: If you are using ‘manual’ certificate revocation via uploading manually a list of expired certificates, do not install any new list from your certificate authority that is dated on or after Feb 1, 2015 until you follow step 3 below.

c. In Cisco Expressway-E or Cisco VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
d. Click **Browse**, select the first certificate that you saved in step a, and click **Open**.
e. Click **Append CA certificate**.
f. Repeat steps d and e for the other certificates you saved in step a.
g. Re-enable 'automatic' certificate revocation, if you disabled it in step b.

Expiration Dates of VeriSign and QuoVadis Certificates

VeriSign Class 3 Public Primary CA - Wednesday, August 02, 2028 3:59:59 PM
VeriSign Class 3 Primary CA - G5 - Wednesday, July 16, 2036
VeriSign Class 3 Public Primary CA - G3 - Wednesday, July 16, 2036 3:59:59 PM
QuoVadis Root CA 2 - November 24, 2031

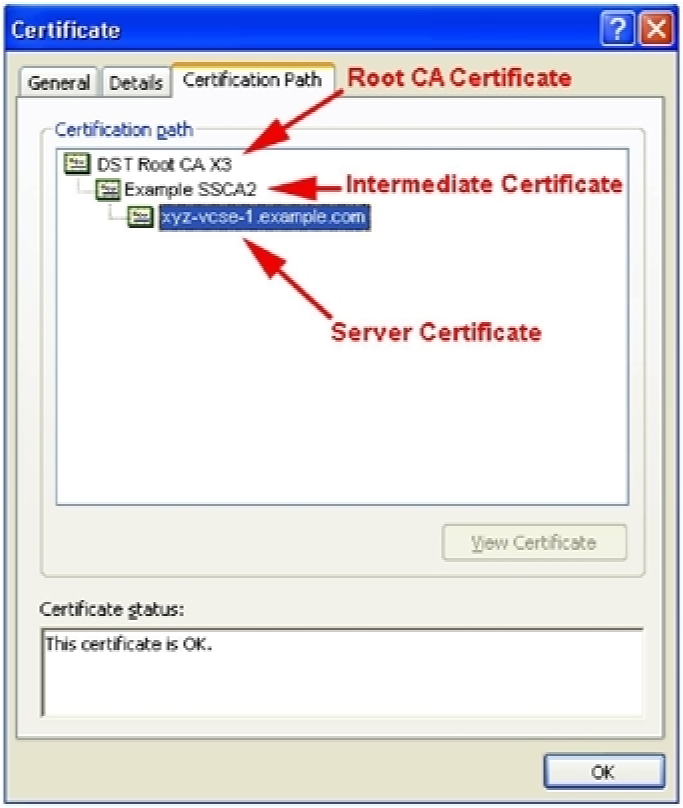
Adding the Root or Intermediate Certificate CA Certificate to Cisco Expressway-E or Cisco VCS Expressway X8.1

For the WebEx cloud to trust the Cisco Expressway-E or Cisco VCS Expressway server certificate, you must add the root or intermediate CA certificate for the CA that issued your server certificate.
Unless the public CA provided you the exact intermediate or root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure that you are stacking the correct intermediate CA certificate.

To add the root or intermediate CA to Cisco Expressway-E or Cisco VCS Expressway X8.1, do the following:
Unless the public CA provided you the exact intermediate and root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure you that you are stacking the correct intermediate CA certificate.

a. Open the server certificate as a .CER file.
b. Click the **Certification Path** tab. (See Figure 17: Server Certificate in .CER File Format [p.90].)

Figure 17: Server Certificate in .CER File Format



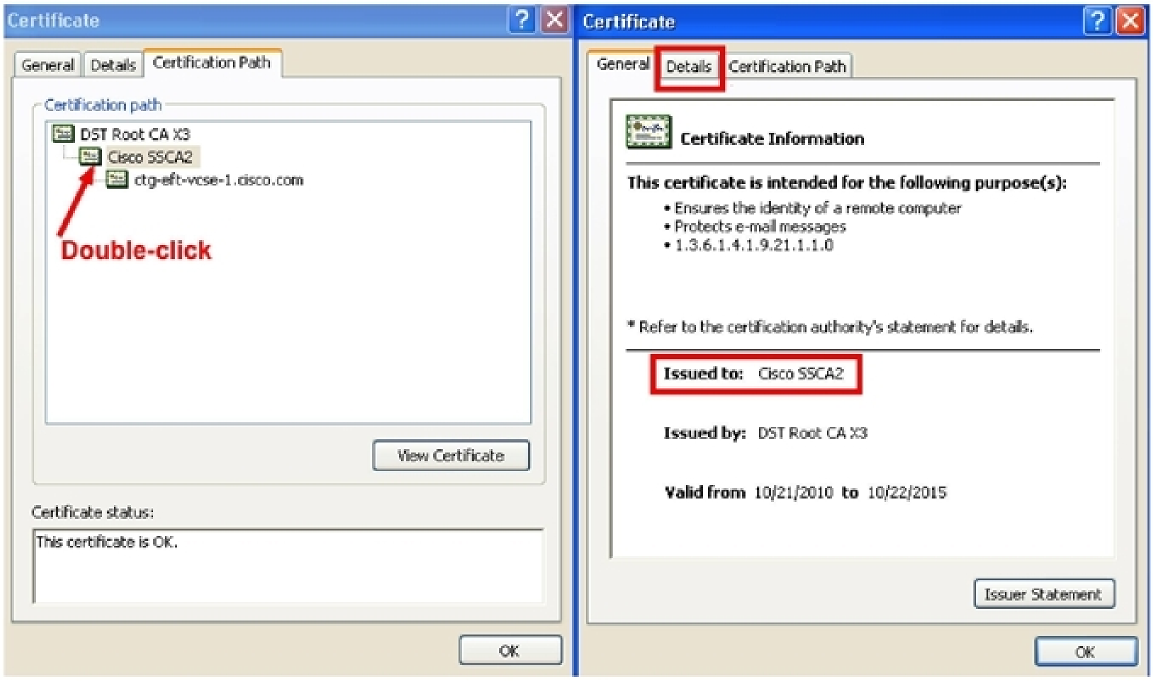
This certificate is OK.

Note: The server certificate example shown here is one issued by an intermediate CA. If your certificate was issued by a root CA, you would only see two certificates (the root and server certificates).

c. Open the CA certificate.
   - If your certificate was issued by a root CA, double-click the Root CA Certificate.
   - If your certificate was issued by an intermediate CA, double-click the Intermediate Certificate.

   This will open the CA certificate in a separate certificate viewer.
d. Make sure the **Issued to** field displays the name of the root or intermediate CA.

e. Click the **Details** tab followed by **Copy to File…**



Certification path

- DST Root CA X3
  - Cisco SSCA2
    - ctg-eft-vcse-1.cisco.com

Certificate status:

This certificate is OK.

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Protects e-mail messages
- 1.3.6.1.4.1.9.21.1.1.0

* Refer to the certification authority's statement for details.

Issued to: Cisco SSCA2

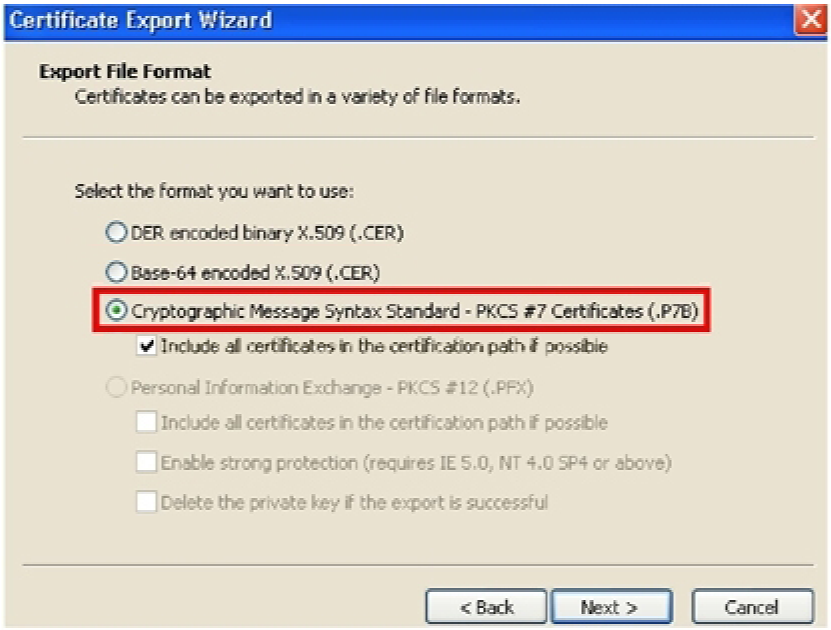
Issued by: DST Root CA X3

Valid from 10/21/2010 **to** 10/22/2015

The **Welcome to the Certificate Export Wizard** appears.

f. Click **Next**.

g. Choose *Cryptographic Message Syntax Standard* as the Export File Format, check *Include all certificates in the certification path if possible* and click **Next**.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☑ Include all certificates in the certification path if possible

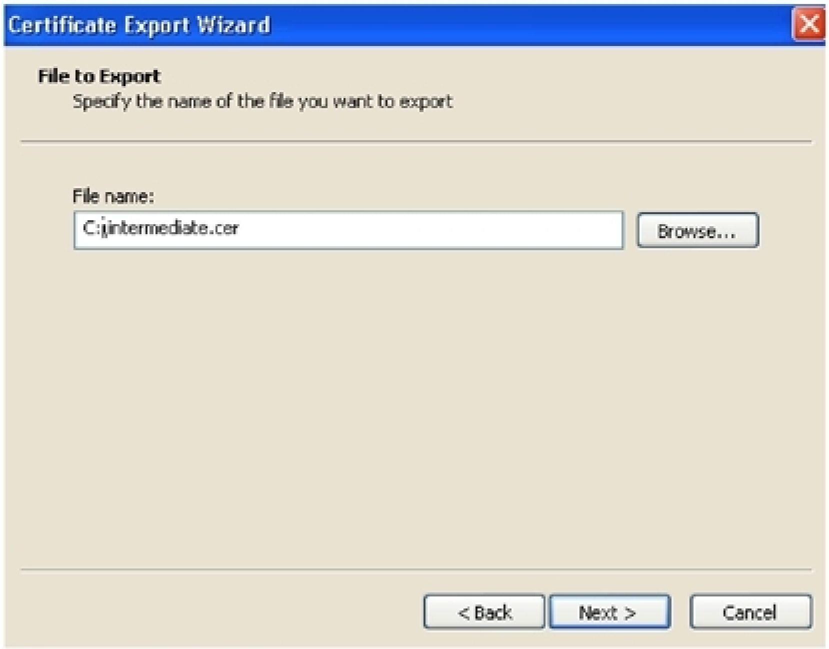
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

h. Name the file, click **Next**, and then click **Finish**.


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\intermediate.cer
Browse...
< Back
Next >
Cancel

i. In Cisco Expressway-E or Cisco VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
j. Click **Browse**, find your root or intermediate CA certificate, and click **Open**.
k. Click **Append CA certificate**.
Certificate configuration on Cisco Expressway-E or Cisco VCS Expressway X8.1 is complete.

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to *Cisco VCS Certificate Creation and Use Deployment Guide (X8.1)* at the following location:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf

Configuring the Trusted CA Certificate List on Cisco Expressway-E or Cisco VCS Expressway X8.1 or Later

Because a freshly installed Cisco Expressway-E or Cisco VCS Expressway X8.1 or later does not have certificates in its trusted CA certificates list, you must add the following certificates:

- The certificates used during the client/server SSL Handshake with the WebEx cloud. See the next section Updating Certificates on Cisco Expressway-E or Cisco VCS Expressway for details.

IMPORTANT: In the past, WebEx used a certificate that was issued under the Root CA ’DST Root CA X3’ to secure traffic between the customer premises and WebEx. We are revoking that certificate and replacing it with new certificates. Your Expressway-E or VCS Expressway MUST trust the new root certificate authorities in order support the new WebEx certificates. If these certificates are not in your Trusted CA list, TelePresence calls may fail to join.

- The CA certificate of the CA that issued your server certificate. See Adding the Root or Intermediate Certificate CA Certificate to Cisco Expressway-E or Cisco VCS Expressway for details.

Updating Certificates on Cisco Expressway-E or Cisco VCS Expressway X8.1

Your Cisco Expressway-E or Cisco VCS Expressway must trust the certificate issuer of the server certificates that are passed by the server during the client/server SSL Handshake with the WebEx cloud. In order to do this, you must add these certificates to the trusted CA list on your Cisco Expressway-E or Cisco VCS Expressway.

To add these certificates to the trusted CA certificate list, do the following:

1. Go to each of the following links, copy and paste the contents of the displayed certificate into individual text files and save each with the file extension of .PEM:
   a. VeriSign Class 3 Public Primary CA
   b. VeriSign Class 3 Primary CA - G5
   c. VeriSign Class 3 Public Primary CA - G3
   d. QuoVadis Root CA 2

   For example, the first one would be:
   `Class-3-Public-Primary-Certification-Authority.pem`

   Note: If you are NOT using Certificate Revocation or do NOT have a Certificate Revocation policy active on your VCS-Expressway or Expressway-E device, skip to step 3.

2. If you are using ‘automatic’ certificate revocation, temporarily disable it:
   a. On the VCS/Expressway, go to: **Maintenance >Security certificates > CRL Management**
   b. Set automatic CRL updates to *disabled*

   Note: If you are using ‘manual’ certificate revocation via uploading manually a list of expired certificates, do not install any new list from your certificate authority that is dated on or after Feb 1, 2015 until you follow step 3 below.

3. In Cisco Expressway-E or Cisco VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
4. Click **Browse**, select the first certificate that you saved in step 1, and click **Open**.
5. Click **Append CA certificate**.
6. Repeat steps 4 and 5 for the other certificates you saved in step 1.
7. Re-enable 'automatic' certificate revocation, if you disabled it in step 2.

Expiration Dates of VeriSign and QuoVadis Certificates

VeriSign Class 3 Public Primary CA - Wednesday, August 02, 2028 3:59:59 PM
VeriSign Class 3 Primary CA - G5 - Wednesday, July 16, 2036
VeriSign Class 3 Public Primary CA - G3 - Wednesday, July 16, 2036 3:59:59 PM
QuoVadis Root CA 2 - November 24, 2031

Adding the Root or Intermediate Certificate CA Certificate to Cisco Expressway-E or Cisco VCS Expressway X8.1

For the WebEx cloud to trust the Cisco Expressway-E or Cisco VCS Expressway server certificate, you must add the root or intermediate CA certificate for the CA that issued your server certificate.

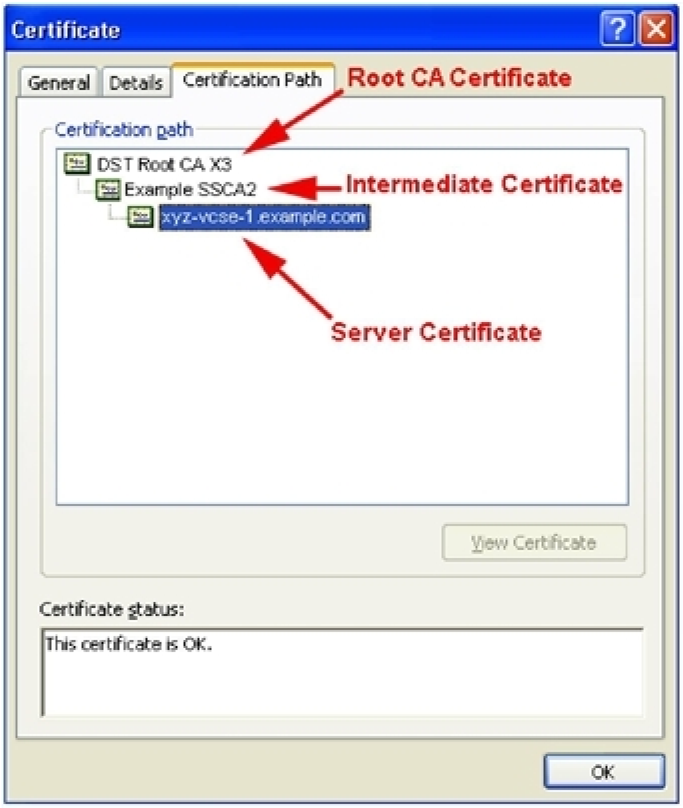
Unless the public CA provided you the exact intermediate or root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure that you are stacking the correct intermediate CA certificate.

To add the root or intermediate CA to Cisco Expressway-E or Cisco VCS Expressway X8.1, do the following:

Unless the public CA provided you the exact intermediate and root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure you that you are stacking the correct intermediate CA certificate.

1. Open the server certificate as a .CER file.
2. Click the **Certification Path** tab. (See Figure 18: Server Certificate in .CER File Format [p.94].)

   Figure 18: Server Certificate in .CER File Format

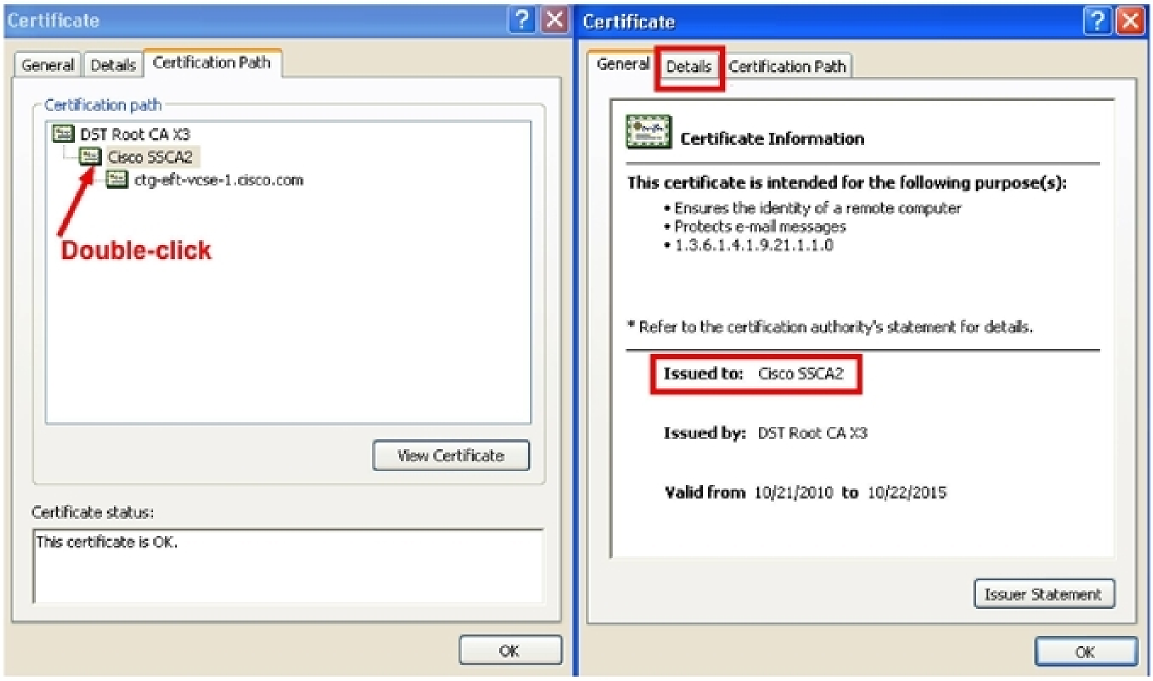
   

   Note: The server certificate example shown here is one issued by an intermediate CA. If your certificate was issued by a root CA, you would only see two certificates (the root and server certificates).

3. Open the CA certificate.
   - If your certificate was issued by a root CA, double-click the Root CA Certificate.
   - If your certificate was issued by an intermediate CA, double-click the Intermediate Certificate.

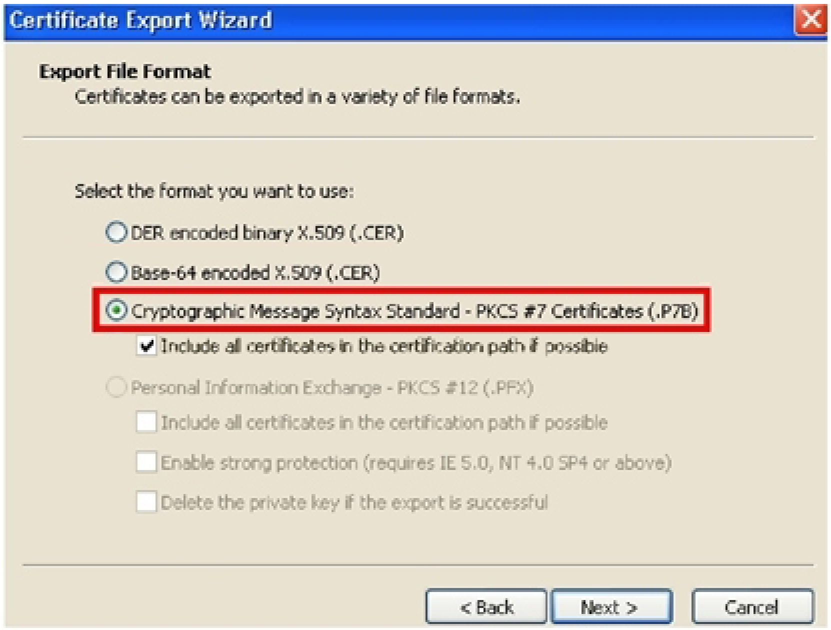
This will open the CA certificate in a separate certificate viewer.

4. Make sure the **Issued to** field displays the name of the root or intermediate CA.
5. Click the **Details** tab followed by **Copy to File…**

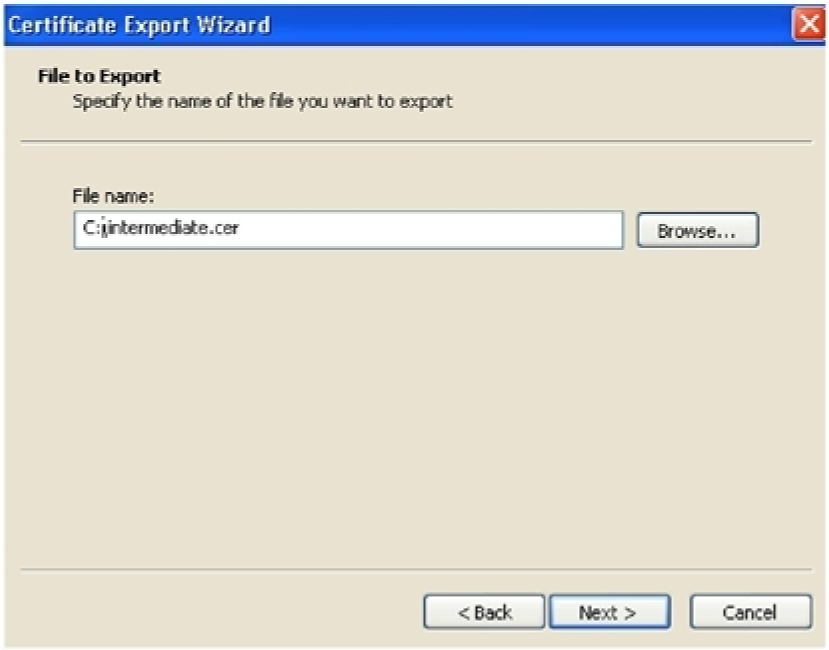


The **Welcome to the Certificate Export Wizard** appears.

6. Click **Next**.
7. Choose *Cryptographic Message Syntax Standard* as the Export File Format, check *Include all certificates in the certification path if possible* and click **Next**.


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
☑ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful
< Back
Next >
Cancel

8. Name the file, click **Next**, and then click **Finish**.



Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name: C:\intermediate.cer

9. In Cisco Expressway-E or Cisco VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
10. Click **Browse**, find your root or intermediate CA certificate, and click **Open**.
11. Click **Append CA certificate**.
    Certificate configuration on Cisco Expressway-E or Cisco VCS Expressway X8.1 is complete.

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to *Cisco VCS Certificate Creation and Use Deployment Guide (X8.1)* at the following location:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf

Configuring Cisco TelePresence Management Suite

First Published: June 23, 2014

This chapter describes how to configure Cisco TMS forCisco Collaboration Meeting Rooms Hybrid meetings. It contains the following sections:

Prerequisites

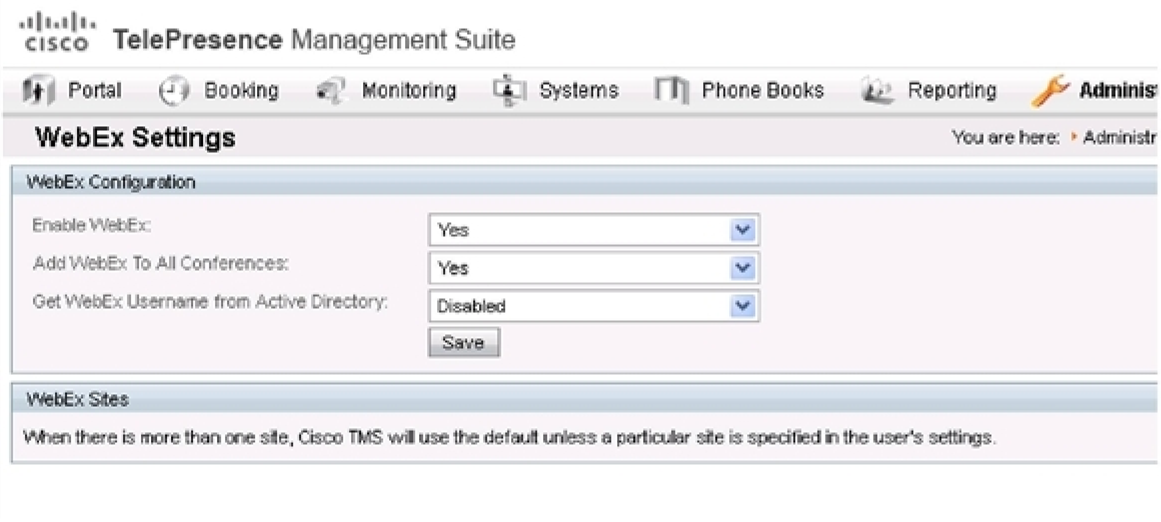
- Cisco TMS software release 14.4 or later is required.
- Cisco TMSXE software release 3.1 or later is required, if using Microsoft Outlook to schedule meetings. There are two options for scheduling using Microsoft Outlook:
  - Using the WebEx Productivity Tools Plug-In for Microsoft Outlook
  - Using WebEx Scheduling Mailbox
- Cisco TMSPE software release 1.1 or later is required, if using Smart Scheduler to schedule meetings
- MCU calls to WebEx support SIP only. The following settings must be configured for SIP:
  - In Cisco TMS: Allow Incoming and Outgoing SIP URI Dialing must be set to **Yes** in the Cisco TMS Scheduling Settings for each MCU used for CMR Hybrid meetings.
  - For MCU and TelePresence Server, see Configuring Cisco TelePresence Management Suite [p.97] for more information.

Configuring the Cisco WebEx Feature in Cisco TMS

To configure the Cisco WebEx feature in Cisco TMS, do the following:

1. Go to **Administrative Tools > Configuration > WebEx Settings**.
   The WebEx Settings page appears.

   Figure 19: Enabling WebEx in Cisco TMS



WebEx Settings

You are here: ‣ Administr

WebEx Configuration

Enable WebEx: Yes
Add WebEx To All Conferences: Yes
Get WebEx Username from Active Directory: Disabled

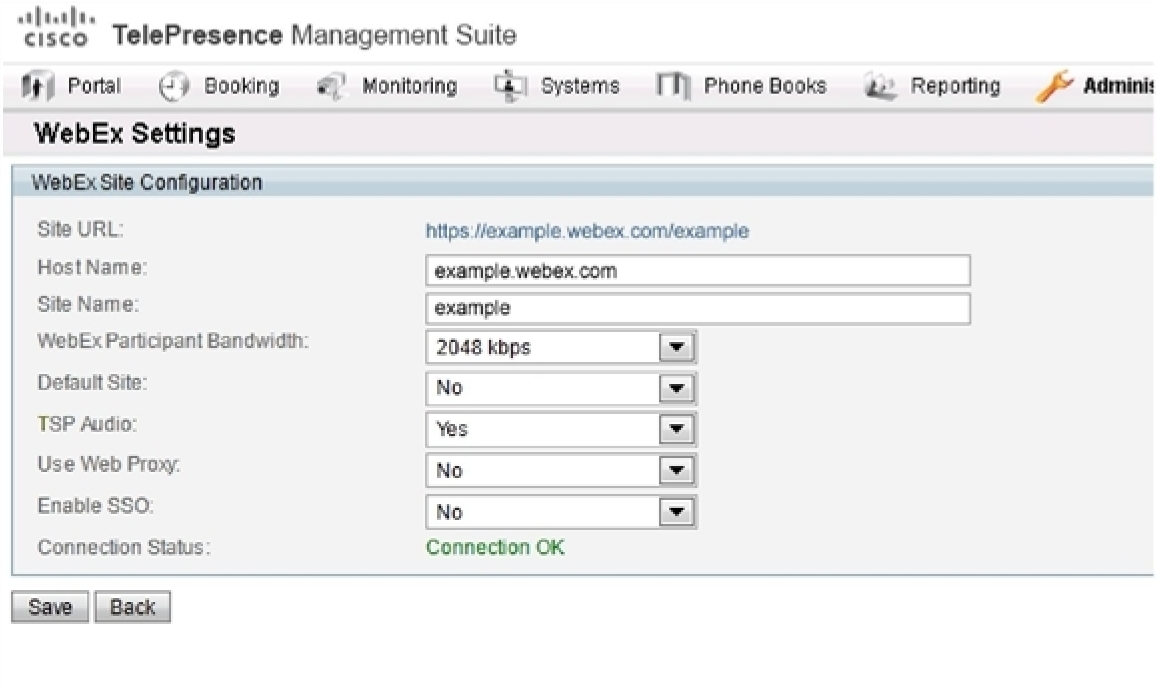
Save

WebEx Sites

When there is more than one site, Cisco TMS will use the default unless a particular site is specified in the user's settings.

2. Click **Add Site**.
   The WebEx Site Configuration page appears.

   Figure 20: Configuring a WebEx Site



WebEx Settings

WebEx Site Configuration

Site URL: https://example.webex.com/example
Host Name: example.webex.com
Site Name: example
WebEx Participant Bandwidth: 2048 kbps
Default Site: No
TSP Audio: Yes
Use Web Proxy: No
Enable SSO: No
Connection Status: Connection OK

Save Back

3. In the **Host Name** field, enter the hostname for the WebEx site.

4. In the **Site Name** field, create a name for the WebEx site.

   Note: The Site URL must follow this format: **`https://[HostName]/[SiteName]`**. For example: **`https://example.webex.com/example`**.

5. For WebEx Participant Bandwidth, select the maximum bandwidth per meeting to allow from MCU to WebEx.

   Note: Bandwidth can be limited in MCU and VCS.

6. (Optional) Default Site. If one or more WebEx sites already exist, you can designate the site as the default WebEx site, by selecting *Yes*.

   Note: New users are automatically set to use the default site the first time they schedule a meeting with WebEx.

7. For **TSP Audio**, select *Yes* if you are going to use TSP or PSTN audio.

   Note: If *Yes* is selected for TSP Audio, Cisco TMS will *only* use TSP audio. SIP audio will *not* work.

8. Click **Save**.
9. In the WebEx Configuration section, do the following:
   a. For **WebEx Enabled**, select *Yes*.
   b. For **Add WebEx To All Conferences**, select *Yes*.
   c. Click **Save**.

Configuring WebEx Users in Cisco TMS

To schedule meetings using Cisco TMS, users must have a username and password that the server is configured to trust.

Cisco TMS authenticates the following accounts:

- Local accounts on the Windows Server where Cisco TMS is installed
- Accounts the server trusts through domain membership and Active Directory (AD)

For each user that successfully logs into Cisco TMS, a new user profile is created based on their username and the user is prompted to enter information into their profile. Existing Windows or AD user passwords are used but they are not stored in Cisco TMS. If a user's Windows/AD password changes, they must use that updated password when logging into Cisco TMS.

User Requirements for Scheduling WebEx-enabled Meetings

To schedule WebEx-enabled meetings using Cisco TMS, Cisco TMS users must have the following stored in their Cisco TMS user profile:

- WebEx username
- WebEx password (unless single sign on is enabled)
- The WebEx site on which they have an account.

Note: This WebEx site must also be added to Cisco TMS, as described in Configuring the Cisco WebEx Feature in Cisco TMS [p.99].

There are three ways to enable a Cisco TMS user's account for WebEx scheduling:

- Administrator edits the Cisco TMS user's profile.
  For details, see Configuring WebEx Users in Cisco TMS [p.101]
- The Cisco TMS user edits their profile by logging in to Cisco TMS and clicking their username at the bottom left corner of the Cisco TMS Web UI.
- Administrator enables ‘Lookup User Information from Active Directory, ‘Get WebEx Username from Active Directory' and (optionally) Single Sign On (SSO).
  The benefits of having the Active Directory lookup features enabled are that the user account information including WebEx username is automatically added to each new Cisco TMS user. WebEx password must still be added by the administrator or user, however, if Single Sign On is enabled, WebEx password is not required. With the Active Directory and Single Sign On features enabled, only the WebEx site must be selected for the user, if there are multiple WebEx sites configured on Cisco TMS. If there is only on WebEx site, Cisco TMS will use that site. If there are multiple sites configured, Cisco TMS will automatically select the WebEx site designated as the ‘Default', unless the user's Cisco TMS profile is edited to specify a different WebEx site.
  For details, see Configuring WebEx Users in Cisco TMS [p.101] and Configuring Single Sign On in Cisco TMS [p.110]

Configuring Automatic User Lookup from Active Directory

If you are using Active Directory (AD), you can configure Cisco TMS to automatically populate user profile information. When you enable this feature, details about the user will automatically be imported when they first access Cisco TMS and synchronized periodically. If you use a field in Active Directory for WebEx username (for example the AD username or email address), you can configure Cisco TMS to import the WebEx username as well by enabling the 'Get WebEx Username from Active Directory' feature in the WebEx Settings page.

Configuring Active Directory Lookup in Cisco TMS

Active Directory Lookup imports and updates user information in Cisco TMS automatically. Optionally, Cisco TMS can also import the WebEx username.

By activating the AD lookup, WebEx and Cisco TMS automatically synchronize user information at given intervals. By doing this, each user of WebEx will only have to enter their password and not their username when booking and entering conferences.

If you do not configure AD lookup, the user will have to enter username and password for communication between Cisco TMS and WebEx.

To configure Active Directory Lookup, do the following:

1. Go to **Administrative Tools** > **Configuration** > **Network Settings**.
2. In the Active Directory pane, set Lookup User Information from Active Directory to **Yes**.
3. Enter information in the remaining fields in the Active Directory pane and click **Save**.
4. For information about each field, refer to the Cisco TMS Help.
5. To configure ‘Get WebEx Username from Active Directory', do the following:
6. Go to **Administrative Tools** > **Configuration** > **WebEx Settings**.
7. In the WebEx Configuration pane, use the Get WebEx Username from Active Directory menu to select the field in AD where you are storing the WebEx username.
8. Click **Save**.

For more information, refer to the Cisco TMS Help.

How WebEx Bookings Work

For WebEx booking to work, the booking user must have a WebEx username and password defined as their WebEx Username and WebEx Password in their Cisco TMS profile. This ensures that the correct user "owns" the meeting in WebEx and can log in and operate the WebEx conference.

When Single Sign On (SSO) is enabled for the WebEx site, users with WebEx accounts can book WebEx-enabled meetings with Cisco TMS without requiring their WebEx password be stored in their Cisco TMS user profile. When SSO is configured and a user schedules a meeting, their WebEx username from their Cisco TMS user profile is passed to the WebEx site to complete the booking. For information about how to configure SSO, see Configuring Single Sign On in Cisco TMS [p.110].

The remaining fields are not mandatory, but are used for other Cisco TMS features. Later, if you are using Active Directory, you can configure Cisco TMS to populate these fields automatically for new users.

Configuring a Cisco CMR Hybrid User in Cisco TMS

This configuration is not required if the following three conditions are true:

- ‘Lookup User Information from Active Directory' and ‘Get WebEx Username from Active Directory' are enabled, as described in Configuring WebEx Users in Cisco TMS [p.101]
- Single Sign On is enabled, as detailed in Configuring Single Sign On in Cisco TMS [p.110].
- The user will use the default WebEx site for scheduling WebEx meetings

To configure a Cisco CMR Hybrid user in Cisco TMS, do the following:

1. Go to **Administrative Tools** > **User Administration** > **Users**
2. Click **New** to add a new user or click the name of an existing user to add WebEx scheduling capabilities to their profile and click **Edit**.
3. Enter Windows/AD Username, First Name, Last Name, and Email Address.

   Note: If an existing user or AD lookup is enabled, some fields will already contain information.

4. For **WebEx Username**, enter the username for the user's WebEx account.
5. For **WebEx Password**, enter the password for the user's WebEx account.

   Note: If no WebEx site is selected, the WebEx site configured as the default will be used.

6. For WebEx Site, select the WebEx site to which the user is registered.
7. Make any other settings in the Cisco TMS user profile and click **Save**.

Configuring Port Reservations for MCU and TelePresence Server in Cisco TMS

Cisco highly recommends configuring MCU and TelePresence Server to reserve ports for each scheduled meeting.

When enabled, the number of ports reserved for the conference is enforced. Therefore if the TelePresence portion of the meeting has 5 ports and 5 participants have joined on TelePresence, if the meeting invitation is forwarded to a 6th person, they will not be able to join the meeting on TelePresence.

If port reservations are not enabled, the meeting is booked with 5 TelePresence ports and the invite is forwarded, additional participants up to the maximum available ports at that time are able to join on TelePresence. This could cause another scheduled meeting to fail. As a result, Cisco recommend s always enabling port reservations for MCU and TS.

Enabling Port Reservations for MCU

To enable port reservations for MCU, do the following in Cisco TMS:

1. Go to **Systems > Navigator**.
2. Select an MCU.
3. Click the **Settings** tab.
4. Click **Extended Settings**.
5. Set the Limit Ports to Number of Scheduled Participants menu to **On**.
6. Click **Save**.
7. Repeat steps 2 through 6 for all other MCUs.

Enabling Port Reservations for TelePresence Server

To enable port reservations for TelePresence Server, do the following in Cisco TMS:

1. Go to **Systems > Navigator**..
2. Select a TelePresence Server system.
3. Click the **Settings** tab.
4. Click **Extended Settings**.
5. Set **Port Reservation** to *On*.
6. Click **Save**.
7. Repeat steps 2 through 6 for every TelePresence Server

Configuring Hybrid Content Mode for MCU in Cisco TMS

Configuring any MCUs that will be used for CMR Hybrid meetings with WebEx to use the hybrid content mode is required. In hybrid mode the incoming content stream is passed through, giving the best possible quality. It is also decoded and used to create a second, lower resolution stream for anyone who cannot receive the passthrough stream. This uses up a video port but ensures that users get the advantages both of transcoding and passthrough.

To configure hybrid content mode on the MCU in Cisco TMS, do the following:

1. Go to **Systems > Navigator**.
2. Select the MCU and click **Edit system settings**.
3. From the **Settings** tab, click **Extended Settings**.
4. For **Content Mode**, select *Hybrid* and click **Save**.

Configuring Lobby Screen TelePresence Server in Cisco TMS

Configuring all TelePresence Servers that will be used for CMR Hybrid meetings with WebEx to set Lobby Screen to “On” is required.

To configure the Lobby Screen on the TelePresence Server in Cisco TMS, do the following:

1. Go to **Systems > Navigator**.
2. Click the TelePresence Server name.
3. Click the **Settings** tab and then click **Extended Settings**.
4. Set "Use Lobby Screen for conferences" to *On* and click **Save**.

How the Lobby Screen Affects the First TelePresence Participant in a Meeting if the WebEx Welcome Screen is Disabled

If the WebEx Welcome Screen is disabled, the user experience of the first TelePresence participant in a meeting that uses TelePresence Server varies depending on how the “Use Lobby Screen for conferences” setting for TelePresence Server is configured in Cisco TMS. Table 17: Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled [p.106] describes what the first TelePresence participant in a meeting will see in different scenarios. To ensure that the first TelePresence participant never sees a black screen, make sure you set “Use Lobby Screen for conferences” to Yes for all TelePresence Servers you will use for CMR Hybrid meetings as described in the previous section.

Table 17: Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled

TelePresence Server Lobby Screen Setting	CMR Hybrid meeting?	At least one WebEx participant?	WebEx participant has camera enabled?	First TelePresence participant will see
No	No. TelePresence only.	N/A	N/A	Black screen (until at least one other TelePresence participant joins)
No	Yes	No	N/A	Black screen (until at least one other TelePresence or WebEx participant joins)
No	Yes	Yes	No	Silhouette image of WebEx participant
No	Yes	Yes	Yes	Video of WebEx participant
Yes	No. TelePresence only.	N/A	N/A	Lobby screen (until at least one other TelePresence participant joins)
Yes	Yes	No	N/A	Lobby screen (until at least one other TelePresence or WebEx participant joins)

Table 17: Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled (continued)

TelePresence Server Lobby Screen Setting	CMR Hybrid meeting?	At least one WebEx participant?	WebEx participant has camera enabled?	First TelePresence participant will see
Yes	Yes	Yes	No	Silhouette of WebEx participant
Yes	Yes	Yes	Yes	Video of WebEx participant

Configuring Conference Settings in Cisco TMS

This section provides information on the recommended and optional conference settings that can be configured in Cisco TMS for CMR Hybrid meetings.

Conference Connection/Ending Options

Cisco recommends configuring the Conference Connection/Ending Options in TMS so that if a meeting runs beyond the scheduled end time, participants are warned if there are not enough resources to extend the meeting.

To configure Conference Connection/Ending Options in Cisco TMS, do the following:

1. Go to **Administrative Tools** > **Configuration > Conference Settings**.
2. In the Conference Connection/Ending Options section, set the following options:
   a. For **Supply Contact Information on Extend Meeting Scheduling Conflict**, select **Yes**.
   This enables participants to see contact information when a meeting extension is not possible, due to a booking conflict.

   Note: This option is not supported by CTS, Jabber Video, and other endpoints that do not support direct messaging from TMS.

   b. For **Show In-Video Warnings About Conference Ending**, select **Yes**.
   TelePresence participants will receive a text message displayed in the video by the bridge, notifying them that the meeting will be ending.
   This feature is compatible with the following bridges:
      - MCU 42xx, 45xx, 84xx, 85xx, 5xxx
      - TelePresence Server 70xx, 87xx
      - Because WebEx is a single participant connection to the MCU/TelePresence Server, the in-video text message will only be visible to WebEx participants when a TelePresence user is the active speaker.

   c. (Optional) You can configure the length, timing and content of the in-video warnings, by setting the following options:
      i. Message Timeout (in seconds): The number of seconds that a warning message will be displayed. Default setting: 10 seconds.
      ii. Show Message X Minutes Before End: The number of minutes before the end of a meeting that the warning message will appear.
      This message can be shown multiple times by separating the minutes with comma. For example **1,5** will display a warning message 1 minute and 5 minutes before the conference ends. Default setting: 1,5 (1 and 5 minutes).
3. Contact Information to Extend Meetings: This field allows you to customize what follows the Meeting End notification. You can enter contact information such as the telephone number or name of a contact person who can extend the meeting for you.
4. The text configured here applies to both the In-Video warnings about conference end sent from bridges to all participants in a conference, and to Meeting End notifications sent to individual participants by Cisco TMS.
5. Click **Save**.

Configuring Allow Early Join

TelePresence participants can join up to 5 minutes before the scheduled start time of the meeting. This ensures that Cisco TMS allocates the conference 5 minutes before the meeting start time on the Main Participant (MCU or TS). This is a best effort feature, so if the Main Participant does not have the resources available, some or all participants may be unable to join the meeting within the 5 minute window.

Note: Cisco TMS does not dial out to WebEx until the scheduled start time of the meeting.

To configure Allow Early Join in Cisco TMS, do the following:

1. Go to **Administrative Tools > Configuration > Conference Settings > Allow Participants to Join 5 Minutes Early**.
2. Click **Save**.

Note: For best results, enable TMS to dynamically increase ports for a meeting above the number selected at the time it was scheduled.

Configuring Resource Availability Check on Extension

When Resource Availability Check on Extension is enabled, a meeting automatically extends by 15 minutes if all resources are available, and reserves them until the extended meeting is finished.

To configure Resource Availability Check on Extension in Cisco TMS, do the following:

1. Go to **Administrative Tools > Configuration > Conference Settings > Resource Availability Check on Extension**.
2. Click **Save**.

This setting works in conjunction with Extend Conference Mode and applies to Automatic Best Effort or Endpoint Prompt. The options are:

- *Best Effort*: Conferences will only automatically extend beyond the scheduled end time on a best effort basis if all resources are available for the next 15 minutes.
- *Ignore*: Cisco TMS will ignore the resource availability check, and conferences will automatically extend beyond the scheduled end time regardless of whether all the resources are available or not. The only exception to this is if the port used on the main participant clashes with another conference.

Configuring Single Sign On in Cisco TMS

Cisco TMS has the option to enable Single Sign On (SSO) for meetings booked by users with WebEx accounts. When SSO is configured and a user schedules a WebEx-enabled meeting, the WebEx username in their Cisco TMS user profile is passed to the WebEx site to complete the booking.

With SSO configured, it is only required to store the user's WebEx username in their Cisco TMS user profile. The user's WebEx password is not required.

There are two ways to add a user's WebEx username to their Cisco TMS user profile:

- A TMS Site Administrator manually enters the WebEx Username in a user's profile.
  When an organizer schedules a meeting with WebEx using Cisco TMS, Cisco TMS sends the meeting information to the WebEx site with that WebEx username designated as the WebEx host.

  Note: When a user has selected a WebEx site that has SSO enabled in TMS, Site Administrator privileges are required to edit the WebEx Username field. Users cannot edit their WebEx Username.

- Enable Cisco TMS to import WebEx usernames from Active Directory (AD)

  Note: You can use any field in AD. Email address and username are the most commonly used.

  When an organizer schedules a meeting with WebEx using Cisco TMS, Cisco TMS requests AD for the WebEx username of the meeting organizer using the username and password that the Cisco TMS administrator filled in on the Network Settings page for AD lookup.
  When AD supplies Cisco TMS with the WebEx username of the organizer, Cisco TMS sends the meeting information to the WebEx site with that WebEx username designated as the WebEx host.

Prerequisites

Before configuring SSO in Cisco TMS, you must work with the WebEx Cloud Services team to determine the following information that needs to be configured in both Cisco TMS and in the WebEx cloud:

- **Partner Name**
  This value must be determined by the WebEx team, because it must be unique among all WebEx customers. Contact the WebEx account team for this information.
  Example: **examplesso.webex.com**
- **Partner Issuer (IdP ID)**
  This is the Identity Provider, which is your TMS. This value must be determined by the WebEx team. Contact the WebEx account team for this information.
  Cisco recommends using a name to indicate your company's TMS.
  Example: **exampletms**
- **SAML Issuer (SP ID)**
  This refers to the Service Provider, which is WebEx. This value must be determined by the WebEx team. Contact the WebEx account team for this information.
  Example: **https://examplesso.webex.com/examplesso**
- **AuthnContextClassRef**
  This is the authentication context. The IdP authenticates the user in different contexts, e.g., X509 cert, Smart card, IWA, username/password).
  Use the default value automatically provided by TMS.

Configuring SSO in Cisco TMS

To configure SSO in Cisco TMS, do the following:

1. Ensure the WebEx site on which you want to enable SSO has been created in Cisco TMS.
   See Configuring the Cisco WebEx Feature in Cisco TMS [p.99] for details.
2. Generate a certificate to secure the connection between Cisco TMS and the WebEx site.
   See Generating a Certificate for WebEx [p.111] for details.
3. Enable Partner Delegated Authentication on the WebEx site.
   See Enabling Partner Delegated Authentication on the WebEx site [p.114] for details.
4. Enable SSO in Cisco TMS.
   See Enabling SSO in Cisco TMS [p.115] for details.

Generating a Certificate for WebEx

WebEx requires that a certificate pair (public certificate and private key) be used to authenticate Cisco TMS to the WebEx cloud.

Certificate pair requirements:

- Public certificate must be in .cer or .crt format - to send to the WebEx Cloud Services team
- Certificate and private key bundled in a PKCS12-formatted file - for upload to Cisco TMS

You can generate a new certificate or use an existing one, such as the one used to enable HTTPS on your Cisco TMS server.

Using an Existing Certificate Signed by a Trusted Authority

If you currently use a certificate signed by a trusted authority, Cisco recommends using the existing certificate and key pair for your WebEx configuration. How you proceed is determined by if the private key is exportable, available or unavailable.

If Private Key is Exportable

If your private key is exportable, do the following:

Using the Windows Certificate Manager Snap-in, export the existing key/certificate pair as a PKCS#12 file.

Using the Windows Certificate Manager Snap-in, export the existing certificate as a Base64 PEM encoded .CER file.

Make sure that the file extension is either .cer or .crt and provide this file to the WebEx Cloud Services team.

Use the PKCS#12 file you created in step 2, to upload to TMS in Configuring Single Sign On in Cisco TMS [p.110]

If Private Key is Not Exportable, but Key/Certificate Pair Available

If your private key is not exportable, but you have the key/certificate pair available elsewhere, do the following:

1. Use Windows Certificate Manager Snap-in to export your existing certificate in a Base64 PEM file.
2. Change the file extension to .cer or .crt and provide the file to the WebEx Cloud Services team.
3. Create a PKCS#12 key/certificate pair by using the command in step 10 of Configuring Single Sign On in Cisco TMS [p.110].
4. Use this PKCS#12 file to upload to TMS in Configuring Single Sign On in Cisco TMS [p.110].

If Private Key is Not Exportable or Available

If your private key is not exportable and it is not available elsewhere, you will need to create a new certificate.

To create a new certificate, follow all the steps in Configuring Single Sign On in Cisco TMS [p.110].

Creating a Key/Certificate Pair Signed by a Certificate Authority

If you do not have a key and certificate pair, but have a certificate authority you use, do the following:

1. Create a new key/certificate pair to use for the WebEx SSO configuration using OpenSSL, following the steps in Configuring Single Sign On in Cisco TMS [p.110].
2. Create a Base64 PEM encoded version of the signed certificate using step 8 Configuring Single Sign On in Cisco TMS [p.110]
3. Change the file extension to .cer or .crt and provide this to the WebEx Cloud Services team.
4. Create a PKCS#12 key/cert pair by using the command in step 10 of Configuring Single Sign On in Cisco TMS [p.110].
5. Use this PKCS#12 file to upload to TMS in Configuring Single Sign On in Cisco TMS [p.110].

Creating a Self-signed Key/Certificate Pair

If you do not have a key and certificate pair and do not have a certificate authority to use, you will need to create a self-signed certificate.

To create a self-signed key, do the following:

1. Follow the steps in Configuring Single Sign On in Cisco TMS [p.110].
2. In step 6, follow the procedure to create a self-signed certificate signing request.
3. Follow steps 7 through 9 generate the base64 PEM file of self-signed certificate, then change the file extension to .cer or .crt and provide it to the WebEx Cloud Services team.
4. Follow step 10 to create a PKCS#12 PFX file
5. Upload to TMS in Configuring Single Sign On in Cisco TMS [p.110].

Using OpenSSL to Generate a Certificate

OpenSSL is an open source project designed to run on Unix and Linux. There is a Windows version available from Shining Light Productions: http://slproweb.com/products/Win32OpenSSL.html. Before using OpenSSL to generate a certificate, you must have OpenSSL installed. For more information, go to: http://www.openssl.org/.

To generate the TMS certificates required for WebEx and TMS, you must complete the following steps:

1. Generate a private key
2. Generate a certificate signing request (CSR)
3. Have a certificate authority sign the CSR

4. Provided the signed certificate in .cer or .crt format to the WebEx team.
5. Convert the signed certificate and private key into a PKCS#12 formatted file
6. Upload the converted certificate and private key to TMS
7. To use OpenSSL to generate a certificate, do the following:
8. In Windows, open a command prompt.
9. Navigate to the openssl\bin installation directory.
10. Generate a private key using following command: **openssl genrsa -out tms-privatekey.pem 2048**
11. Generate a certificate signing request (CSR) using the private key above: **openssl req -new -key tms-privatekey.pem -config openssl.cfg -out tms-certcsr.pem**
12. Enter the data requested, including:
    - Country
    - State or province
    - Organization name
    - Organization unit
    - Common name (this is the Cisco TMS FQDN)
    - (Optional) Email address, password, company name
13. Send the Cisco TMS certificate signing request file **tms-certcsr.pem** to be signed by a trusted certificate authority (CA) or self sign a certificate signing request using OpenSSL or Windows CA.

For details on how to submit a certificate request to a trusted certificate authority, contact that certificate authority.

To self-sign a certificate signing request using OpenSSL, use the following command. **tms-certcsr.pem** is your certificate signing request in PEM format. **tms-privatekey.pem** is your private key in PEM format. **days** is the number of days you'd like the certificate to be valid.

openssl x509 -req -days 360 -in tms-certcsr.pem -signkey **tms-privatekey.pem** -out tms-cert.pem

The resulting **tms-cert.pem** is your self-signed certificate.

To self-sign a certificate signing request using Windows CA, use Windows Certificate Manager Snap-in. For details on how to submit a certificate request using Windows Certificate Manager Snap-in, refer to the documentation for Windows Certificate Manager Snap-in.

When your certificate authority has signed your certificate request, they send a signed certificate to you, You should receive the signed certificate **tms-cert.der** back from the CA.

If the certificate is on an email or web page and not in its own file, copy the contents starting with the -----BEGIN CERTIFICATE----- line and through the -----END CERTIFICATE----- line. Save the contents to a text file and name the file **tms-cert.der**.

Convert the signed certificate from .der to .pem using the following OpenSSL command:

openssl x509 -inform der -in tms-cert.cer -out tms-cert.pem

Note: If the certificate authority provides you the signed certificate in .pem format, you can skip this step.

Change the file extension of the signed certificate to .cer or .crt and provide this signed certificate to the WebEx Cloud Services team.

Combine the signed certificate .pem with the private key created in step 3:

openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -name tms-cert-key

You should now have a Cisco TMS certificate that contains the private key for SSO configuration to upload to Cisco TMS.

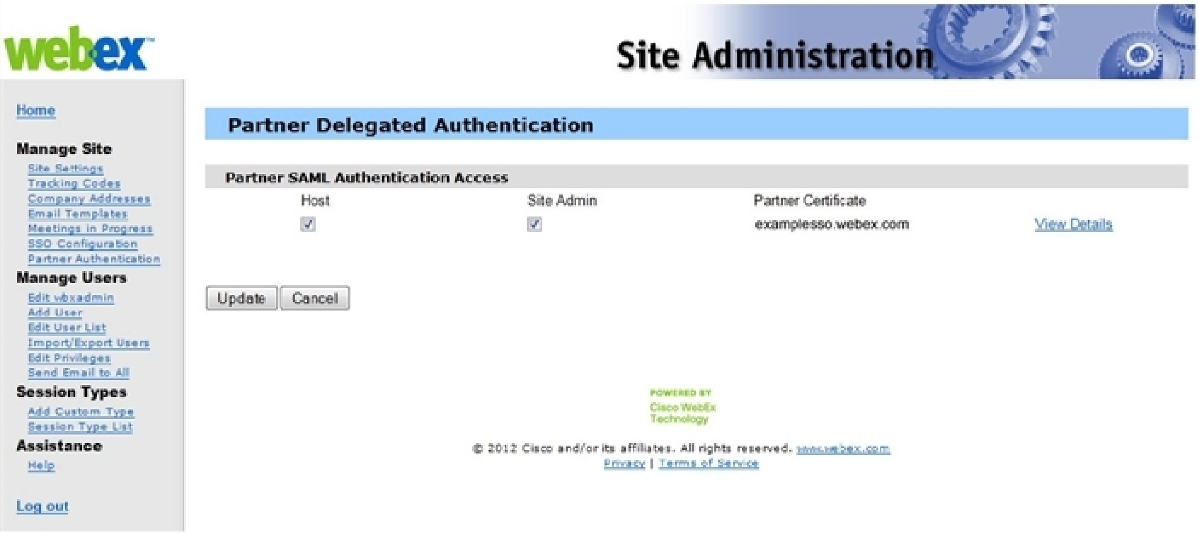
Before uploading this certificate to TMS, you must enable partner delegated authentication on your WebEx site. For more information, refer to Configuring Single Sign On in Cisco TMS [p.110] in the next section. After enabling delegated authentication, use the combined certificate and private key you generated in step 10 above to upload to Cisco TMS in step 4 of Configuring Single Sign On in Cisco TMS [p.110] to complete the SSO configuration.

Enabling Partner Delegated Authentication on the WebEx site

Before you can enable partner delegated authentication on your WebEx site, the WebEx Cloud Services team must make site provisioning changes to configure your TMS as a delegated partner.

These steps are required for enabling partner delegated authentication on your WebEx site:

1. Request that the WebEx Cloud Services team add a Partner Certificate for your TMS, configured for SAML 2.0 federation protocol.
2. Provide the public certificate for your TMS to the WebEx Cloud Services team. For details on how to create a certificate, see Configuring Single Sign On in Cisco TMS [p.110].
3. After the WebEx Cloud Services team notifies you that this step is complete, enable partner delegated authentication for both Host and Admin accounts in the Site Administration for your WebEx site, as described below.
4. Proceed with the section "Enabling SSO in Cisco TMS".
5. To enable partner delegated authentication on your WebEx site, do the following:
6. Log into your WebEx administrative site and go to **Manage Site** > **Partner Authentication**.
7. The Partner Delegated Authentication page appears.
8. Partner Delegated Authentication on the WebEx Administrative Site



Partner SAML Authentication Access

Host	Site Admin	Partner Certificate	
☑	☑	examplesso.webex.com	View Details

9.

10. In the Partner SAML Authentication Access section, make sure both **Host** and **Site Admin** are checked and click **Update**.

Enabling SSO in Cisco TMS

Before you begin, make sure you have the following information:

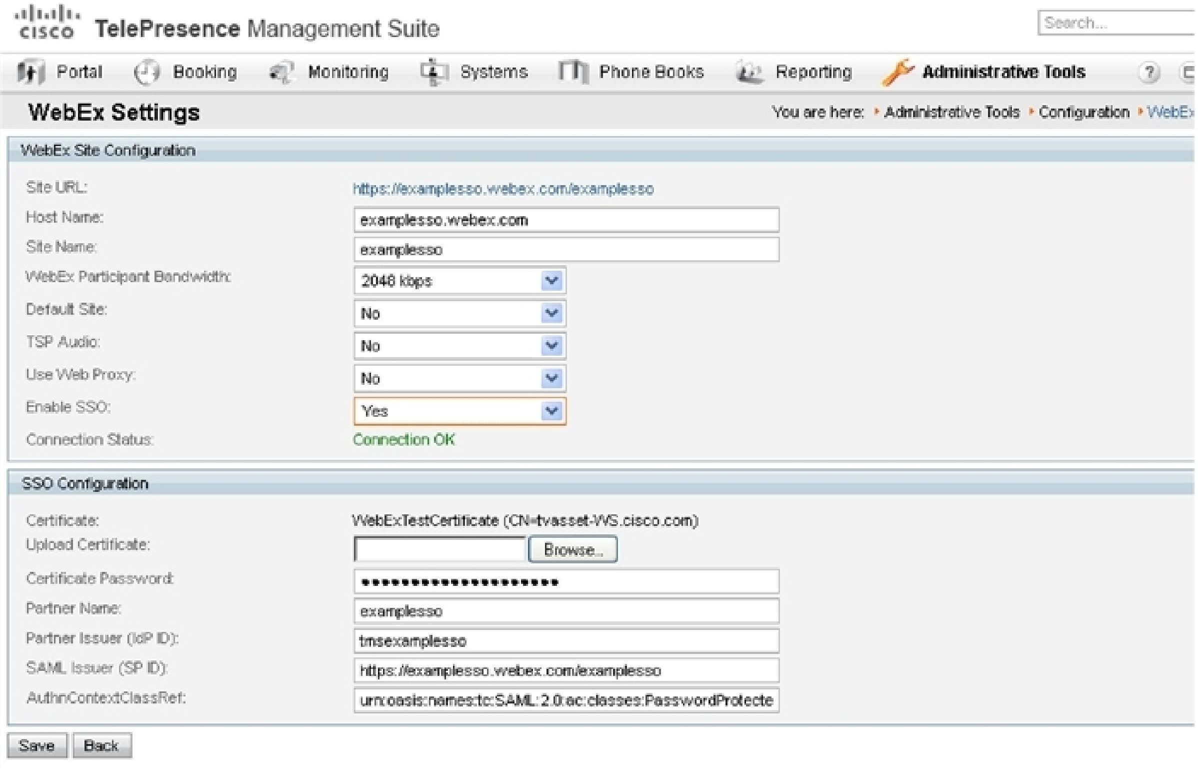
- Certificate Password (if required)
- Partner Name
- Partner Issuer (IdP ID)
- SAML Issuer (SP ID)
- AuthnContextClassRef

Note: Before enabling SSO, you must enable Partner Delegated Authentication on your WebEx site. For more information, refer to Configuring Single Sign On in Cisco TMS [p.110].

To enable SSO in Cisco TMS, do the following:

1. Log into Cisco TMS, and go to **Administrative Tools > Configuration > WebEx Settings**.
2. In the WebEx Sites pane, click the site name of the WebEx site on which you want to enable SSO.
3. The WebEx Site Configuration pane appears.
4. For Enable SSO, select **Yes**.
5. The SSO Configuration pane appears.
6. Click **Browse** and upload the PKS #12 private key certificate (.PFX) you generated in Configuring Single Sign On in Cisco TMS [p.110].
7. Complete the rest of the SSO configuration fields using the password and other information that you selected when generating the certificate.
8. Click **Save**.

Figure 21: WebEx Settings SSO Configuration in Cisco TMS



WebEx Settings

WebEx Site Configuration

Site URL:	https://examplesso.webex.com/examplesso
Host Name:	examplesso.webex.com
Site Name:	examplesso
WebEx Participant Bandwidth:	2048 kbps
Default Site:	No
TSP Audio:	No
Use Web Proxy:	No
Enable SSO:	Yes
Connection Status:	Connection OK

SSO Configuration

Certificate:	WebExTestCertificate (CN=tvasset-WS.cisco.com)
Upload Certificate:	
Certificate Password:	••••••••••••••••••••
Partner Name:	examplesso
Partner Issuer (IdP ID):	tmsexamplesso
SAML Issuer (SP ID):	https://examplesso.webex.com/examplesso
AuthnContextClassRef:	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtecte

Supported Configurations for Cisco TMS to Schedule on Behalf of the WebEx Host

While the focus of the previous section was how to configure SSO on TMS, it is also possible to configure SSO on the WebEx site itself. As a result, it's helpful to understand all the supported configurations for scheduling of CMR Hybrid meetings.

There are three possible supported configurations to allow the TMS to schedule on behalf of the WebEx host:

- WebEx site does not use SSO and TMS does not have SSO configured (no partner delegated authentication relationship with the WebEx site)
  - WebEx host login: The WebEx username and password are stored in WebEx, and the user authenticates directly to the WebEx site.
  - TMS scheduling: The host's WebEx username and password are also stored in their TMS personal profile. This must be maintained by the user, if they have access to the TMS, or by the TMS administrator. The TMS passes both username and password to WebEx at scheduling time.
- WebEx site does not use SSO, but TMS does have SSO configured (partner delegated authentication relationship with the WebEx site).
  - WebEx host login: The WebEx username and password are stored in WebEx, and the user authenticates directly to the WebEx site.
  - TMS scheduling: The host's WebEx username is stored in a TMS personal profile (a TMS admin task) but the WebEx password is not stored in TMS. TMS is trusted to schedule for that user.

- WebEx site uses SSO, and TMS has SSO configured (partner delegated authentication relationship with the WebEx site).
  - WebEx host login: The WebEx user logs in through the SSO identity service provider.
  - TMS scheduling: The host's WebEx username is stored in a TMS personal profile (a TMS admin task) but the WebEx password is not stored in Cisco TMS. Cisco TMS is trusted to schedule for that user.

Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange

First Published: June 23, 2014

This chapter describes how to configure Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE) for scheduling of CMR Hybrid meetings using the WebEx and TelePresence Integration to Outlook and WebEx Scheduling Mailbox. It contains the following sections:

Prerequisites

- Cisco TMSXE software release 3.1 or later is required.
- Cisco TMS software release 14.4 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 4GB 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 Installation Guide - Version 3.1

Scheduling Options with Cisco TMSXE

With Cisco TMSXE, there are two options for scheduling CMR Hybrid:

- Using the WebEx Productivity Tools Plug-In for Microsoft Outlook
  You add WebEx to your meeting using WebEx Meeting Options panel in Microsoft Outlook.
- Using WebEx Scheduling Mailbox
  You add WebEx to your meeting invitation directly from your email client by including a special invitee; the WebEx mailbox.

Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook

To configure Cisco TMSXE for scheduling using the WebEx and TelePresence Integration to Outlook, you must perform the following tasks:

- Install the Cisco TMS Booking Service
- Set up communication between your WebEx site and TMSXE

Installing the Cisco TMS Booking Service

To allow WebEx Productivity Tools with TelePresence to communicate with Cisco TMSXE you must have Booking Service installed.

If you did not include the proxy during initial installation, do the following:

1. On the Cisco TMSXE server, go to the Control Panel.
2. Right-click **Cisco TelePresence Management Suite Extension for Microsoft Exchange** and select **Change**.
3. This starts the installer and allows you to change your installation.
4. Follow all instructions provided by the installer and opt to include Cisco TMS Booking Service.

Note: Installing the Booking Service forces a restart of IIS.

Configuring IIS for HTTPS

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

If IIS is not present on the server prior to installation of Cisco TMSXE, it will be 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.

In the IIS configuration 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.

Configure 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):

1. Open the Server Manager console (Start > All Programs > Administrative Tools > Server Manager).
2. In the Role View, select IIS Manager (Server Manager > Roles > Web Server > IIS Manager).
3. Double-click **Server Certificates**.

4. In the Actions pane on the right, click **Create Certificate Request**.
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.
6. In the "Organization" field, type your organization name.
7. In the "Organizational Unit" field, type the name of your organization and click **Next**.
8. In the "City/locality" field, type the city where the server resides and click **Next**.
9. In the "State/province" field, type the state where the server resides.
10. In the "Country/Region" field, select US (United States) and click **Next**.
11. Leave the CSP at the default value.
12. For the "Bit Length", select 2048.
13. Enter (or Browse to) a filename to save the certificate request (CSR), click **Finish**.
14. Copy and paste the entire contents of the CSR file you just saved.
    The default save location is C:\.
15. Provide the CSR file to your CA and wait for them to send a signed certificate back to you.
16. Installing the Public Root Certificate in IIS7 (Windows Server 2008):
17. Double-click the **Root CA** certificate file and click **Install Certificate**.
18. Click **Next**, place the radio button in **Place all certificates in the following store** and then click **Browse**.
19. Place a check in **Show Physical Stores**.
20. Expand the **Trusted Root Certification Authorities** folder, select the **Local Computer** folder, and click **OK**.
21. Click **Next** and then **Finish**. You will receive the message: "The import was successful".

Installing the Intermediate CA certificate (if applicable):

1. Double-click the **Intermediate CA** certificate file and click **Install Certificate**.
2. Click **Next**, place the radio button in **Place all certificates in the following store** and then click **Browse**.
3. Place a check in **Show Physical Stores**.
4. Expand the **Intermediate Certification Authorities** folder, select the **Local Computer** folder, and click **OK**.
5. Click **Next** and then **Finish**. You will receive the message: "The import was successful".

Installing your SSL server certificate:

1. In the IIS Manager console, go to the **Server Certificates** action pane, and click **Complete Certificate Request**. The Complete Certificate Request Wizard appears.
2. Browse to the location where you saved your SSL server certificate, select it, then click **Open**.
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.
4. In the action pane on the right, under Edit Site, click **Bindings**.
5. Click the **Add** button.
6. In the Type menu, select **https**.

7. In the SSL certificate menu, select your SSL certificate.
8. Click **OK**.

Setting Up Communication Between Your WebEx Site and Cisco TMSXE

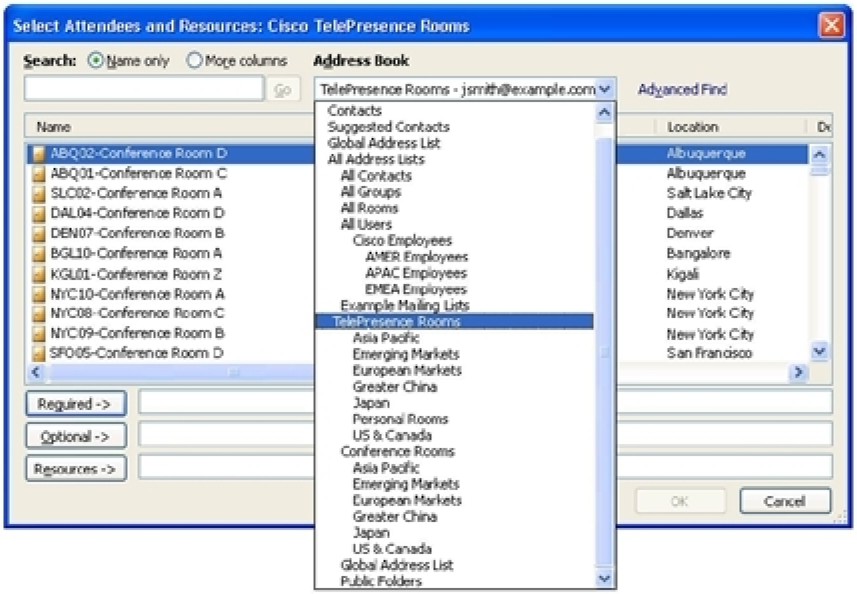
Follow the steps described in Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.150].

Configuring the Location Displayed for TelePresence Rooms in Outlook

When selecting telepresence rooms while scheduling a CMR Hybrid meeting in Outlook, the location of the room is displayed in the both the Select Attendees and Resources Address Book window (Figure 22: Select Attendees and Resources - Address Book [p.124]), which is a standard part of Outlook, and the Select Telepresence Rooms window (Figure 23: Select TelePresence Rooms [p.125]), which is displayed when using the WebEx and TelePresence Integration to Outlook.

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

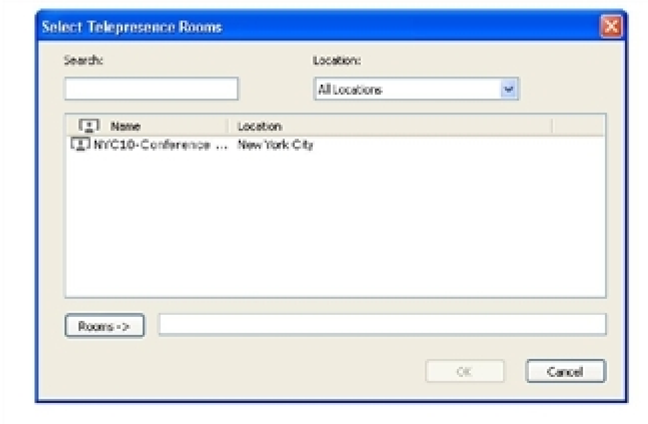
Figure 22: Select Attendees and Resources - Address Book



Name	Location
ABQ02-Conference Room D	Albuquerque
ABQ01-Conference Room C	Albuquerque
SLC02-Conference Room A	Salt Lake City
DAL04-Conference Room D	Dallas
DEN07-Conference Room B	Denver
BGL10-Conference Room A	Bangalore
KGL01-Conference Room Z	Kigali
NYC10-Conference Room A	New York City
NYC08-Conference Room C	New York City
NYC09-Conference Room B	New York City
SFO05-Conference Room D	San Francisco

- To display the Add Telepresence Rooms window, click the **Add Telepresence Rooms** button the Meeting Options pane.

Figure 23: Select TelePresence Rooms



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 the WebEx and TelePresence Integration to Outlook. 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 the WebEx and TelePresence Integration to Outlook [p.122] Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook [p.122].

The structure and hierarchy displayed in the drop-down menu in the Exchange Address Book (Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook [p.122]) 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.

Installing the WebEx and TelePresence Integration to Outlook

Meeting organizers who want to schedule meetings using the WebEx and TelePresence Integration to Outlook plug-in, must download and install the WebEx Productivity Tools with TelePresence from your WebEx site. For details, refer to: Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.150]

Configuring Cisco TMSXE for the WebEx Scheduling Mailbox

To configure Cisco TMSXE for scheduling using the WebEx Scheduling Mailbox, you must do the following procedures:

1. Configure the WebEx mailbox in Microsoft Exchange.
2. Add the WebEx mailbox to Cisco TMSXE.

Configuring the WebEx Scheduling Mailbox in Microsoft Exchange

To configure the WebEx mailbox in Microsoft Exchange, use either Exchange Management Console or Powershell:

1. Create a new user mailbox for your WebEx Scheduling Mailbox *(example: webex@example.com)*.
   For more information, refer to: Create a Mailbox (Exchange 2010 Help) or How to Create a Mailbox for a New User (Exchange 2007 Help).
2. Give the EWS Service Account Full Mailbox Access to this mailbox.
   For more information, refer to: Allow Mailbox Access (Exchange 2010 Help) or How to Allow Mailbox Access (Exchange 2007 Help).
3. Modify mailbox properties:
   a. Turn off the Calendar Attendant for the mailbox.
      For more information, refer to: Configure User and Resource Mailbox Properties (Exchange 2010 Help) or How to Disable the Auto-Processing of Meeting Messages (Exchange 2007 Help).
   b. Make sure new requests are not automatically marked as tentative by disabling **AddNewRequestsTentatively (Mark new meeting requests as Tentative)** if using the Calendar Settings tab) for the mailbox.

Adding the WebEx Mailbox to Cisco TMSXE

To add the WebEx Mailbox to Cisco TMSXE, do the following:

1. Log in to the server on which TMSXE is installed.
2. From the Windows task bar, select **Start** > **All Programs** > **Cisco** > **TMSXE Configuration**.
3. If Cisco TMSXE is already running, a message appears indicating you must stop the Cisco TMSXE service to start the configuration tool. Click **Stop Service**.
   The Cisco TMSXE Configuration window appears.
4. Click the **Exchange Web Services** tab.
5. In the WebEx Scheduling Mailbox field at the bottom of the window, enter the email address of the WebEx mailbox you created in Microsoft Exchange.
6. Click **Save**.
   TMSXE validates the email address you provided and a message appears indicating your settings have been saved.
7. Click **Exit**.

Additional Recommendations

Cisco also recommends using the following configurations for WebEx Scheduling Mailbox:

- Using Exchange Management Console Mail Flow Settings or Powershell, stricken the message delivery restrictions as needed.
  For example, require senders to be authenticated, only allow from people in a specific group or similar.
  For more information, refer to: Configure Message Delivery Restrictions (Exchange 2010 Help) or How to Configure Message Delivery Restrictions (Exchange 2007 Help).
- Using AD Users and computers or Powershell, set the Active Directory user account to disabled.
  See Disable or Enable a User Account for instructions.

Configuring Cisco TelePresence Management Suite Provisioning Extension

First Published: June 23, 2014

This chapter describes how to configure Cisco TelePresence Management Provisioning Extension (Cisco TMSPE) for scheduling of CMR Hybrid meetings using Smart Scheduler. It contains the following sections:

Prerequisites

- Cisco TMS software release 14.4 or later must be installed.
- Cisco TMSPE software release 1.1 or later must be installed and enabled in Cisco TMS.
- WebEx must be configured on Cisco TMS.
  - Cisco WebEx option key
  - One or more WebEx sites
  - Single sign-on or specified WebEx credentials for each user.
    Cisco highly recommends that Single Sign On is configured for Cisco TMS and WebEx for easy addition and management of users.

    Note: If Single Sign On is not configured In Cisco TMS, you must manually add a WebEx username and password for each Cisco TMS Smart Scheduler user that will schedule meetings with WebEx.

    For details on how to configure Cisco TMS, see Configuring Single Sign On in Cisco TMS [p.110].
- Smart Scheduler requires one of the following browsers:
  - Microsoft Internet Explorer - version 10 or later
  - Mozilla Firefox - version 29 or later
  - Apple Safari - version 7 or later for Mac OS X and iPad
  - Google Chrome - version 34 or later

Introduction

Smart Scheduler is a part of the Cisco WebEx and TelePresence solution, allowing users to schedule telepresence meetings with WebEx.

With Smart Scheduler users can schedule Cisco TelePresence meetings with and without WebEx.

Any bookable system in Cisco TMS can be scheduled directly. Any system that is not supported by Cisco TMS booking can be scheduled as a call-in participant, including devices provisioned by Cisco TMSPE.

The option to include WebEx in a meeting is available in the Smart Scheduler booking form if Cisco WebEx has been set up with Cisco TMS.

Note: The default date and time format for a new meeting is **dd.mm.yyyy** and **24-hour** time format. Each user can change these default settings by clicking their name or the wrench icon in the upper-right portion of the Smart Scheduler window. This setting is saved as a cookie in the each browser used.

User Access to Cisco TMSPE

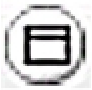
Users with the necessary credentials can reach Smart Scheduler using:

http://<Cisco TMS Server Hostname>/tms/booking/

Example: http://example-tms.example.com/tms/booking/

Users who already use Cisco TMS can also click the portal icon in the upper right corner to go to Smart Scheduler and FindMe.

Figure 24: Cisco TMS Portal Icon



Creating a Redirect to Smart Scheduler

It is also possible to create an HTTP redirect using the following HTML code:

```
<html>
       <head>
               <META HTTP-EQUIV="Refresh" CONTENT="0; URL= https://<Cisco TMS Server
Hostname>/tmsagent/tmsportal/#scheduler">
               <title>Cisco TelePresence Management Suite Smart Scheduler</title>
       </head>
       <body>
       </body>
</html>
```

Access Rights and Permissions

Access to Smart Scheduler works the same as access to Cisco TMS.

Users must have one of the following accounts:

- A local account on the Cisco TMS Windows Server
- A domain account that the server trusts through Active Directory. By making the server a member of the domain, all trusted domain users can automatically use their existing Windows credentials.

A Cisco TMS user account will be created for them when they access the site if one does not exist already.

Note: The actual booking is not created directly by the individual user, but on their behalf by the Cisco TMSPE service user added during installation. Booking permissions will therefore be the same for all users.

Time Zone Display

Bookings are created using the time zone of the user's web browser (determined by the time zone of the user's operating system).

Within the scheduler itself, the time zone of the web browser and operating system is displayed.

How Smart Scheduler Works

1. When a domain user signs into Smart Scheduler and books a meeting, the request is passed to Cisco TMS.
2. This communication goes through the Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA).
3. The Cisco TMS user entered during installation of Cisco TMSPE is the service user for Smart Scheduler. This user creates the booking in Cisco TMS on behalf of the Cisco TMSPE user.
4. If the Cisco TMSPE user does not already exist in Cisco TMS, it will be created at the same time as the booking.
5. When the booking is complete, Cisco TMS sends an email confirmation to the user who booked the meeting. The message containing meeting details including route, scheduled systems, WebEx information, and so on, may then be forwarded to the other meeting participants.

Limitations

Cisco strongly recommends that meetings scheduled in Cisco TMS not be modified using Smart Scheduler, as this interface and does not support all features and options that may have been chosen for the meeting in Cisco TMS.

- Exceptions to recurrent meeting series are not supported in Smart Scheduler. Any modification will be applied to all instances.
- Smart Scheduler will rename call-in participants added from Cisco TMS.

Configuring Audio

First Published: June 23, 2014

This chapter describes how to configure audio for Cisco Collaboration Meeting Rooms (CMR) Hybrid.

Prerequisites

To configure SIP or PSTN Audio, the following are required:

- Cisco VCS Control/Cisco VCS Expresswaymust be configured.
  For details, refer to: Configuring Cisco Expressway and TelePresence Video Communication Server [p.61].
- When using Unified CM, make sure:
  - SIP trunk is configured between Unified CMand Cisco VCS Control.
  For details, see Configuring Cisco Unified Communications Manager [p.64]
  - Your regions are configured for G.711 and G.722.
- If configuring PSTN audio, Gateway must be registered to Cisco VCSor Unified CM.
- MCUs/TelePresence Servers must be registered to VCS.
  - No support for MCUs/TelePresence Servers trunked to Unified CM.
- Endpoints registered to VCS and/or Unified CM and able to call into MCUs/TelePresence Servers
- Familiarity with all of required products
- If configuring TSP audio and the TSP provider offers a waiting room feature, the TSP provider must configure it to allow multiple hosts to log in to the audio conference, or the human host must be trained to not log in as a host. If multiple hosts are not enabled, each host that dials in disconnects the host that dialed in before it. For example, if the MCU dials in first, when the human host dials in later, they will disconnect the MCU.
  The human host still maintains host privileges on the WebEx client and can mute/unmute participants through that user interface if needed.

  Note: Cisco TelePresence Conductor is not supported at this time.

- If configuring TSP audio, the TSP provider must support the Call-in User Merge feature. Call-in User Merge allows TSP partners to pass the attendee ID via DTMF code, rather than prompting the user via the audio. The WebEx Meeting Manager prompts the user to enter the DTMF code, followed by the attendee ID.

Configuring SIP Audio for CMR Hybrid

The following section describes the steps required for configuring SIP audio for CMR Hybrid.

This section describes the following:

- Configuring the WebEx Site in Cisco TMS to Use SIP Audio [p.137]
- Enabling Hybrid Audio on the WebEx Site [p.137]

Note: SIP audio only supports WebEx audio (TSP audio is not supported).

Configuring the WebEx Site in Cisco TMS to Use SIP Audio

To configure Cisco TMS to use SIP for the WebEx site, do the following:

1. Log into Cisco TMS.
2. Go to **Administrative Tools** > **Configuration** > **WebEx Settings**.
3. The **WebEx Settings** page appears.
4. Click the name of the WebEx site you want to configure.
5. The **WebEx Site Configuration** page appears.
6. If a new site, enter the Site Name, Host Name, and other required fields.
7. For TSP Audio, select **No**.
8. Click **Save**.

Enabling Hybrid Audio on the WebEx Site

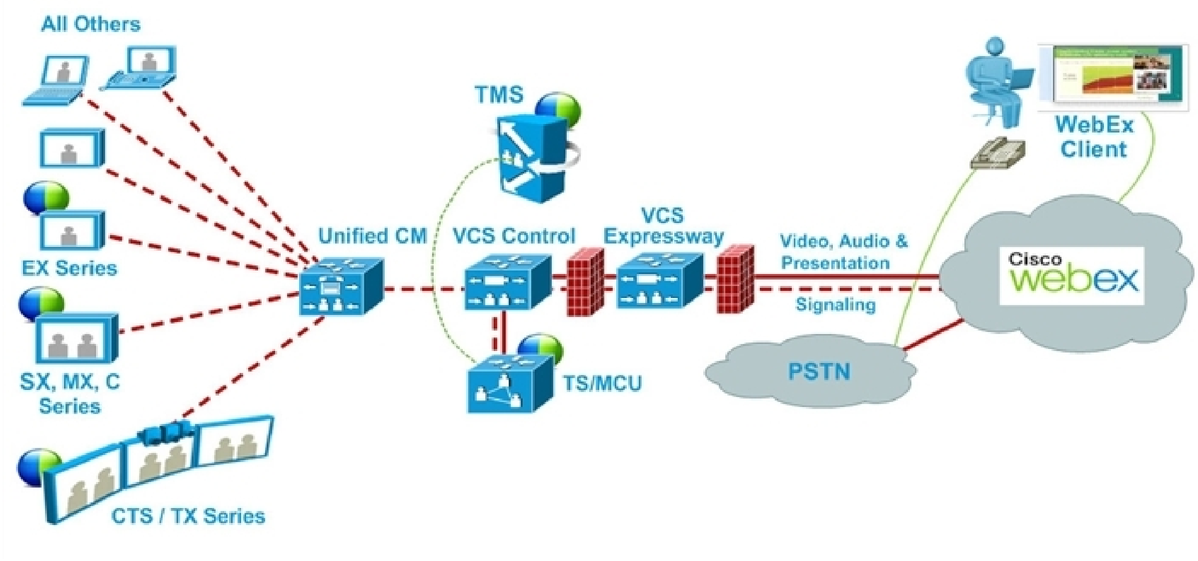
To use SIP audio, your WebEx site must be enabled for **Hybrid Audio**. Hybrid Audio is also required to provide your WebEx participants the option of using their computer to connect to the audio portion of a meeting.

This configuration must be done by the WebEx team. Contact the WebEx team for assistance, or submit an online ticket at:

https://cisco-support.secure.force.com/WebEx_GPL_WebForm

Hybrid Audio is required when using TelePresence Server as the conference bridge in a meeting, because it only supports SIP audio at this time.

Figure 25: SIP Audio Deployment with Endpoints Registered to Unified CM



Configuring PSTN Audio for CMR Hybrid

The following section describes the steps required for configuring PSTN audio for CMR Hybrid.

This section describes the following:

- Configuring the WebEx Site in Cisco TMS to Use PSTN Audio [p.139]
- Enabling Hybrid Mode on the WebEx Site [p.139]
- Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx [p.139]

Note: Cisco CMR Hybrid always dials a fully qualified E.164 number beginning with the international escape character (+). For example: `+14085551212`. Make sure that VCS and/or Unified CM call routing is set up accordingly.

Configuring the WebEx Site in Cisco TMS to Use PSTN Audio

To configure Cisco TMS to use PSTN for the WebEx site, do the following:

1. Log into Cisco TMS.
2. Go to **Administrative Tools** > **Configuration** > **WebEx Settings**.
3. The WebEx Settings page appears.
4. Click the name of the WebEx site you want to configure.
5. The WebEx Site Configuration page appears.
6. If a new site, enter the Site Name, Host Name and other required fields.
7. For TSP Audio, select *Yes*.
8. Click **Save**.

CAUTION: If the meeting organizer chooses a TelePresence Server when scheduling the meeting, Cisco TMS will automatically attempt to schedule the meeting using MCU. If an MCU is not available, the meeting will not be scheduled successfully.

Enabling Hybrid Mode on the WebEx Site

If you want WebEx participants to have the option of using their computer to join the audio portion of a meeting, your WebEx site must be set to **Hybrid** mode. This configuration must be done by the WebEx team. Contact the WebEx team for assistance.

Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx

WebEx always provides a fully qualified E.164 number beginning with the international escape character (+). For example: +14085551212. VCS and/or Unified CM call routing must be properly configured to ensure PSTN calls are routed correctly.

Two deployments models are supported for routing PSTN calls to pass through a PSTN gateway to WebEx:

- Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco VCS [p.140]
- Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Unified CM [p.141]

Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco VCS

To configure PSTN calls to pass through a PSTN Gateway registered to VCS, do the following:

On VCS, create a transform or search rule that transforms the globally routable number provided by WebEx (example: +14085551212) to a number with the tech-prefix of the gateway registered to VCS (example: 9#14085551212).

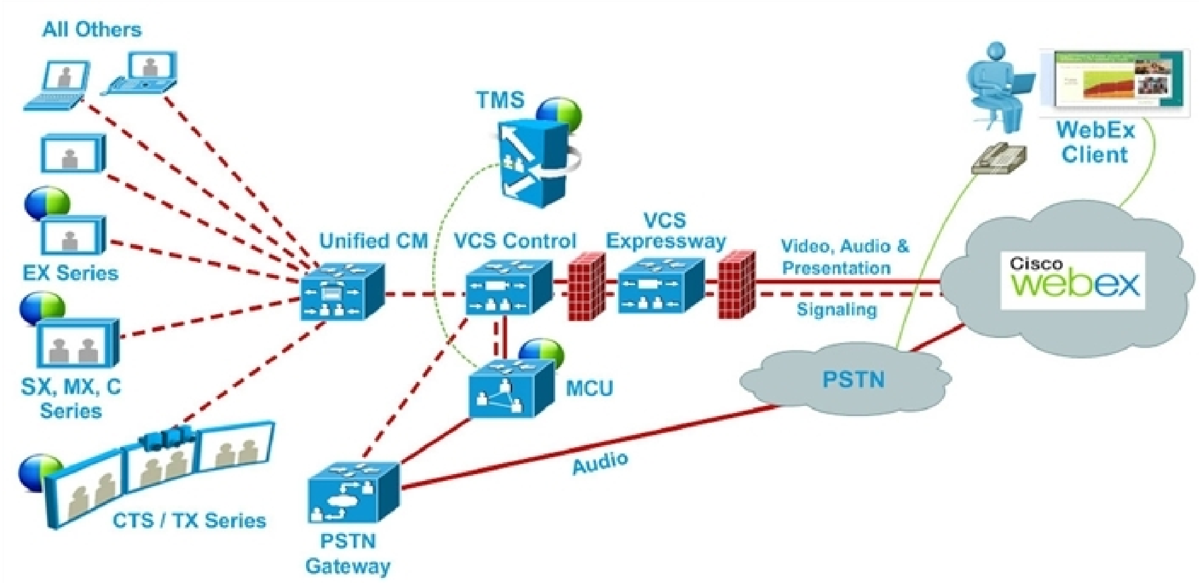
This example transforms **`+14085551212@example.webex.com`** to **`9#14085551212@example.webex.com`** using the Regex pattern type:

- Pattern string: **`\+(\d+@.*)`**
- Replace string: **`9#\1`**

For more information about configuring traversal zones, search rules and transforms in VCS, refer to *Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide*:

https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf

Figure 26: PSTN Audio Deployment with Gateway Registered to VCS and Endpoints Registered to Unified CM



Configuring Cisco VCS Control for ISDN Gateways

If you are going to use an ISDN gateway to pass PSTN calls through to WebEx, you must configure the Interworking setting in Cisco VCS Control.

Note: This step is required only for ISDN gateways.

To configure Cisco VCS Control for ISDN Gateways, do the following:

1. Log in to Cisco VCS Control.
2. Go to **VCS Configuration** > **Protocols** > **Interworking**.
3. For H.323 <-> SIP interworking mode select **On** and click **Save**.

Note: An option key is required in order to save this configuration.

Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Unified CM

To configure PSTN calls to pass through a PSTN Gateway registered to Unified CM, do the following:

1. On VCS, create a search rule that takes the globally routable number with the international escape character (+) provided by WebEx (example: `+14085551212`) and routes it to Unified CM.
2. On Unified CM, create a route pattern according to your dial plan to route these types of calls to the appropriate PSTN gateway registered to Unified CM.

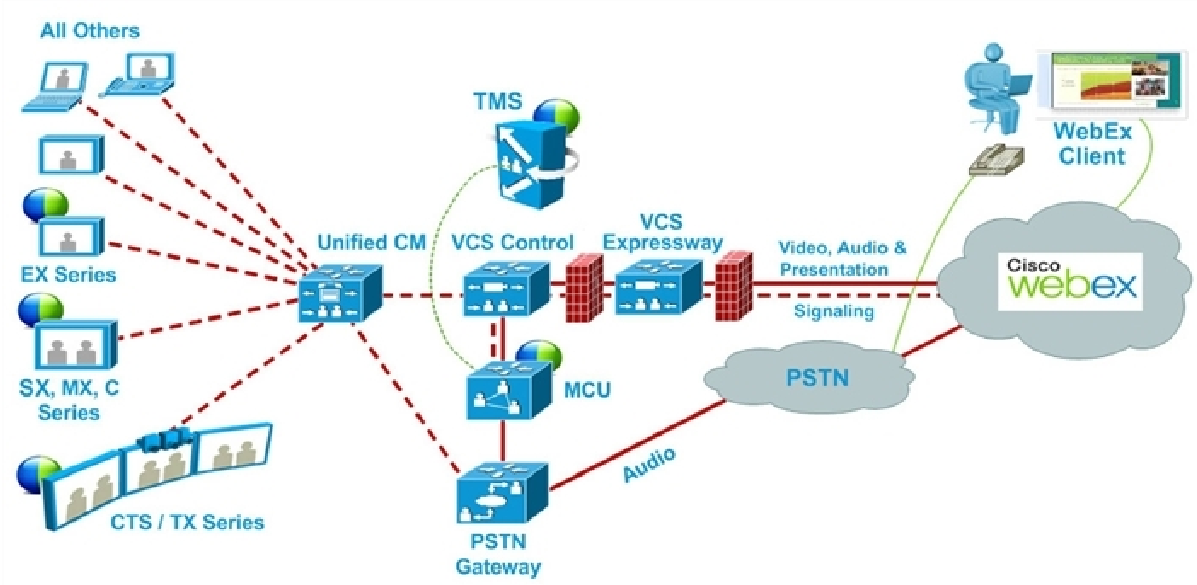
For more information about configuring search rules on VCS, see *Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide*:

https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf

For more information about configuring route patterns in Unified CM, refer to the documentation for your Unified CM version:

https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Figure 27: PSTN Audio Deployment with Gateway and Endpoints Registered to Unified CM



Configuring TSP Audio for CMR Hybrid

To deploy Telephony Service Provider (TSP) audio, PSTN audio is required. Follow the steps in Configuring PSTN Audio for CMR Hybrid [p.139] and then contact WebEx cloud services to assist you with the TSP configuration.

For VCS-centric deployments, you must enable BFCP in the Unified CM neighbor zone on Cisco VCS. If BFCP is not enabled, the TelePresence conference may fail to join the WebEx conference.

There are four required parts to TSP audio configuration:

- Configuring MACC Domain Index and Open TSP Meeting Room WebEx Settings [p.142]
- Configuring the TSP Dial String [p.142]
- Configuring How the Conference is Opened [p.143]
- Configuring TSP Audio for the Meeting Organizers [p.145]

For more information, see:

- Overview of TSP Audio Configuration and Meetings [p.146]

Note: TSP audio requires that the MCU/TS is able to make an outbound call to establish an audio cascade between TelePresence and the TSP partner audio bridge. To ensure that the MCU/TS can make the call, see Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco VCS [p.140].

Configuring MACC Domain Index and Open TSP Meeting Room WebEx Settings

WebEx cloud services must configure these settings for you. Contact WebEx cloud services for more information.

Configuring the TSP Dial String

To connect to a meeting that uses TSP audio, the telepresence equipment dials into the TSP partner's audio bridge and navigates the interactive voice response (IVR) audio prompt menu hierarchy by using DTMF tones. Each TSP provider uses a different set of IVR menu prompts. As a result, your TSP audio provider must create and test a static DTMF dial string for your meetings, and then provide the string to Cisco WebEx cloud services. Cloud services then configures the dial string parameters in the WebEx cloud for your WebEx site.

Note: If the TelePresence phone call to the TSP audio service will be over a SIP trunk, that SIP trunk must be able to carry in-band DTMF. If the SIP trunk cannot carry in-band DTMF, call routing for the TelePresence outbound calls should be adjusted so they do not use the SIP trunk. This is because the TelePresence phone call to the TSP issues in-band DTMF signals (the TelePresence Server does not support RFC 2833 for transmitting).

DTMF Dial String Example

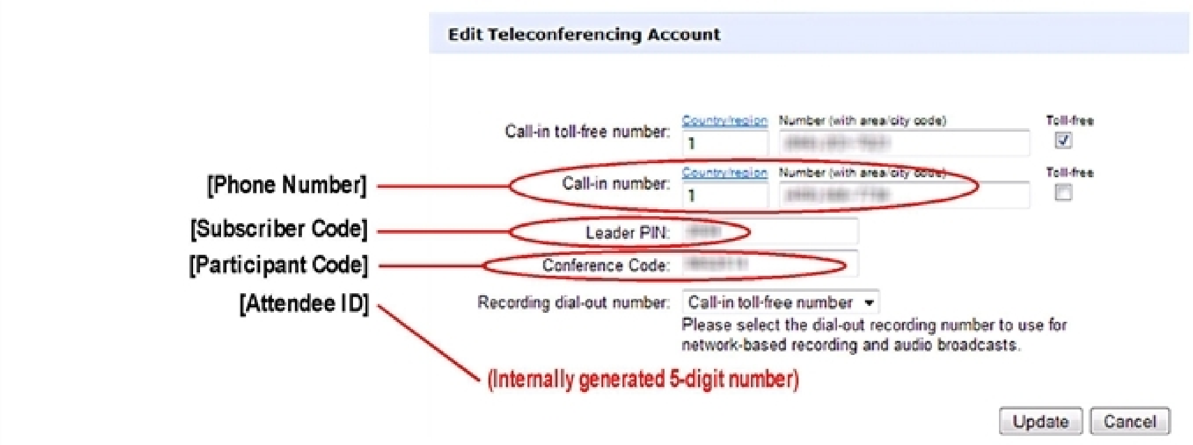
The following is an example of a sequence that a TSP provider might use to generate a DTMF dial string:

1. Dial the phone number
2. Pause 2 seconds
3. Enter [participant code] DTMF values (Example: 12345678)
4. Enter #
5. Pause 6 seconds
6. Enter #
7. Pause 25 seconds
8. Enter #1
9. Pause 1 second
10. Enter [attendee ID] DTMF values (Example: 44356)

Variables Available to the Dial String

The following variables are available for use with the DTMF dial string that is created by your TSP audio provider and configured by WebEx cloud services.

Figure 28: WebEx Host Account / TSP Audio Account



Edit Teleconferencing Account

Call-in toll-free number: Country/region 1 Number (with area/city code) [redacted] Toll-free ☑

Call-in number: Country/region 1 Number (with area/city code) [redacted] Toll-free □

Leader PIN: [redacted]

Conference Code: [redacted]

Recording dial-out number: Call-in toll-free number ▾

Please select the dial-out recording number to use for network-based recording and audio broadcasts.

[Phone Number]
[Subscriber Code]
[Participant Code]
[Attendee ID]
(Internally generated 5-digit number)

For more information on the DTMF dial string, contact Cisco WebEx cloud services.

Configuring How the Conference is Opened

TSP providers typically wait for the WebEx host to call in before opening up an audio conference for the meeting.

Until the host dials in (by entering the host access key) participants wait in a waiting room. If the host is late or never dials in and unlocks the meeting from WebEx, the meeting never starts.

Contact your TSP provider to determine if they have a waiting room. If they do have a waiting room, there are two methods for ensuring the conference is opened for a meeting:

- **Method 1**: WebEx cloud services works with the TSP provider to include the host access key in the DTMF dial string used by the MCU/TelePresence Server.
  - As soon as the first telepresence participant joins the meeting, the MCU/TelePresence Server dials the string and joins as the host, unlocking the meeting.
  - Because the MCU/TelePresence Server dials in to the TSP on behalf of the host, the provider must

configure the audio conference to allow multiple hosts to log in. Otherwise, if a human host dials in after the MCU/TelePresence Server dials in, the bridge is disconnected. The bridge then redials and the human host is disconnected.
With multiple hosts, the human host still retains host privileges in the Cisco WebEx Meeting Center application, and can mute or unmute participants or perform other host functions through the Meeting Center if needed.

- If the WebEx host enters the meeting before the first telepresence participant joins, participants hear the DTMF dial string when the MCU/TelePresence Server attempts to start the meeting.
- For situations where the host hangs up while the meeting is still underway, the audio conference may terminate, depending on the TSP implementation and whether the hosts selects the option to keep the meeting running in the Meeting Center application upon leaving.

Note: A DTMF dial string is required, whether or not you include the host access key in the string. Contact WebEx cloud services for more information.

- **Method 2**: The WebEx TSP server sends the **W2A_UpdateConference=2** API command to the TSP partner's bridge to unlock the meeting.
  - The TSP partner may have to recode their TSP adapter in order to recognize and properly execute the unlock conference command.
  - For situations where the host hangs up while the conference is still underway, the partner should keep the conference running until either all attendees have left the conference or the TSP API sends **W2A_CloseConference**.

  Contact your TSP provider to determine if they support the API command method.

With either method, if the host joins the meeting and uses the Meeting Center to lock the meeting before the first telepresence participant joins, the MCU/TelePresence Server may fail to join the audio conference.

Impacts of the TSP Meeting Start Method

The following table describes common scenarios and the impact on the meeting experience depending on which method is used to start the meeting from the waiting room.

Table 18: Scenarios and Results for TSP Methods

Scenario	Expected result	If method 1 is used	If method 2 is used
MCU/TelePresence Server is the first caller into the audio conference	Successful join	The MCU/TelePresence Server will have host role in the TSP audio conference.	The MCU/TelePresence Server will not have the host role in the audio conference.
One or more attendees have already joined the audio conference (waiting room) before the MCU/TelePresence Server dials in.	Successful join	The MCU/TelePresence Server will have host role in the TSP audio conference	The MCU/TelePresence Server will not have the host role in audio.

Table 18: Scenarios and Results for TSP Methods (continued)

Scenario	Expected result	If method 1 is used	If method 2 is used
The host has already joined the audio conference before the MCU/TelePresence Server dials in.	Successful join	Users who have already joined the audio conference may hear the "extra" DTMF tones broadcast into the audio conference, which is the MCU/TelePresence Server following the DTMF sequence as though it were the host.	No such extra DTMF tones will be heard.
The host (who had already joined the audio conference before the MCU/TelePresence Server dials in), hangs up while the conference is still underway.	Varies	Audio conference may terminate. Depends on TSP implementation - some may not terminate. Depends on host's selection in WebEx GUI upon leaving conference (option to keep conference running)	Since method 2 is being used, the partner should keep the conference running until either: ■ all attendees have left the conference or ■ TSP API sends W2A_ CloseConference
DTMF failure	Fail to join		
The host joins via WebEx before the MCU/TelePresence Server dials in, and the host uses the WebEx GUI to lock the conference. (WebEx has decided to respect the hosts' locking of the conference in this case.)	Fail to join	The MCU/TelePresence Server should fail to join	The MCU/TelePresence Server should fail to join

Configuring TSP Audio for the Meeting Organizers

Each meeting organizer who needs to schedule CMR Hybrid meetings that use TSP audio must log in to the WebEx site and configure their account to use TSP audio. This is a one-time configuration.

Enabling the WebEx Site for Creation of TSP accounts

WebEx site administrator must enable WebEx site to allow creation or editing of a TSP account:

1. Log in to WebEx Site Administration for the WebEx site
2. Under **Manage Site** > **Site Settings** > **Default Scheduler Options**, check **Allow creating or editing TSP account**.
3. Click **Update**.

Configuring TSP Audio for the Meeting Organizer

The meeting organizer must have the following information, provided by the TSP audio service provider:

- Call-in toll-free number
- Call-in number
- Host access code
- Attendee access code

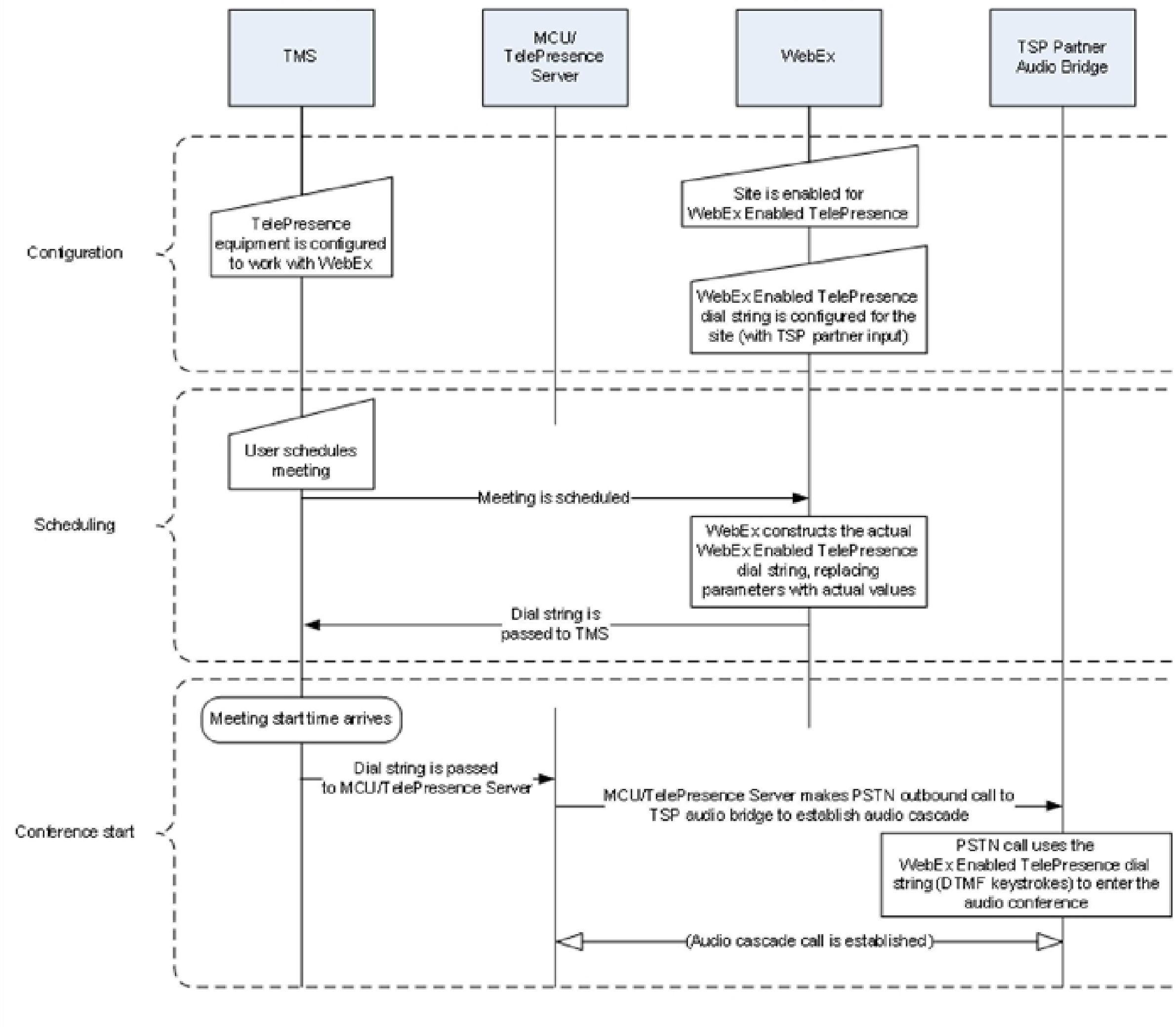
To configure TSP audio, instruct each meeting organizer to do the following:

1. Open a browser and go to your WebEx site. (Example: *http://example.webex.com*)
2. In the upper part of the page, click **My WebEx**.
3. (If necessary) Enter the **Username** and **Password** for your WebEx account and click **Log In**.
4. In the left-hand side of the page, click **Preferences**.
5. Click the **Audio** preference.
6. Add Teleconferencing account including the appropriate phone numbers and access codes for the host and attendees, as provided by the TSP audio service provider. For details, refer to the WebEx Site Administration guide available on your WebEx site.

Overview of TSP Audio Configuration and Meetings

The following diagram provides an overview of which components are configured for TSP audio, as well as what takes place when a meeting is scheduled and starts.

Figure 29: TSP Audio Configuration, Scheduling and Meeting Start Flow


TMS
MCU/ TelePresence Server
WebEx
TSP Partner Audio Bridge
Configuration
TelePresence equipment is configured to work with WebEx
Site is enabled for WebEx Enabled TelePresence
WebEx Enabled TelePresence dial string is configured for the site (with TSP partner input)
Scheduling
User schedules meeting
Meeting is scheduled
WebEx constructs the actual WebEx Enabled TelePresence dial string, replacing parameters with actual values
Dial string is passed to TMS
Conference start
Meeting start time arrives
Dial string is passed to MCU/TelePresence Server
MCU/TelePresence Server makes PSTN outbound call to TSP audio bridge to establish audio cascade
PSTN call uses the WebEx Enabled TelePresence dial string (DTMF keystrokes) to enter the audio conference
(Audio cascade call is established)

How a TSP Meeting Works

A meeting that uses TSP Audio takes place the following way:

1. The meeting is scheduled.
2. A dial string is passed back to the MCU/TelePresence Server.
3. At the scheduled start time, the MCU/TelePresence Server starts the meeting.
4. TelePresence connects into WebEx via SIP.
5. The TSP partner starts the audio conference on their bridge and they open up the conference.
6. At the same time as TelePresence connects to WebEx via SIP, it also dials via PSTN into the TSP partner bridge using the DTMF dial string.

Behavior of TSP Audio Meetings When the MCU or TelePresence Server Dials in as Host

The MCU/TelePresence Server will attempt to redial the connection for any reason up to a maximum number of retries. In the case where the MCU/TelePresence Server joins as host, it is important to note that if the MCU/TelePresence Server is the host and this call is disconnected for any reason, the TSP partner may tear down the audio conference (all participants may be disconnected). The MCU/TelePresence Server will immediately dial back in and re-establish the audio conference, but the participants may need to call back in again. The word "may" is used here because we understand this to be configurable on the TSP and/or the behavior may differ from one TSP provider to another.

Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account

First Published: June 23, 2014

This chapter describes how to configure your WebEx site for CMR Hybrid. It contains the following sections:

Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account

You have access to the Cisco WebEx Site Administration interface 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 Cisco TelePresence system.

Proceed to the following sections to complete first-time setup:

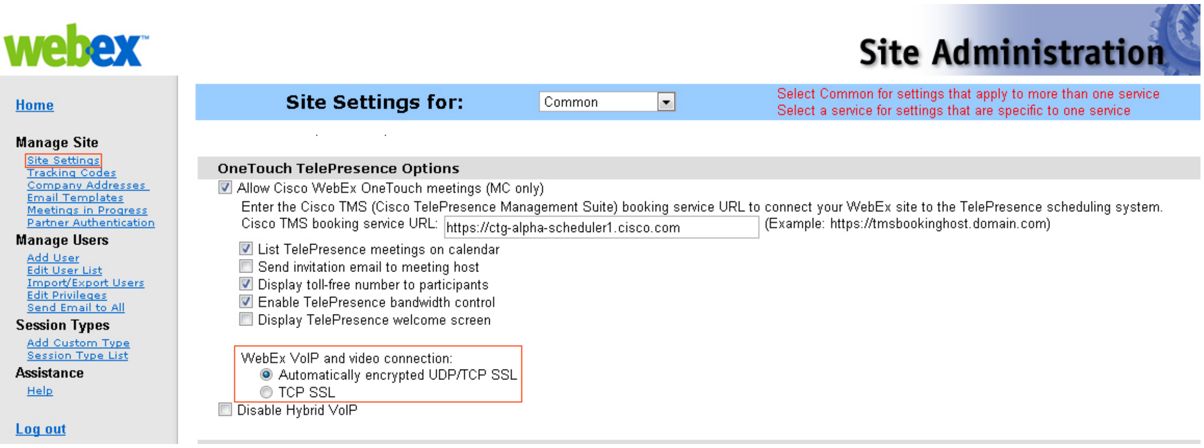
- Configuring Cisco WebEx Site Administration for CMR Hybrid [p.150]
- Assigning the Meeting Center TelePresence Session Type [p.152]

Configuring Cisco WebEx Site Administration for CMR Hybrid

To integrate Cisco TelePresence to Cisco WebEx:

1. Log in to the WebEx Site Administration interface using your WebEx Site Administration URL username and password.
   This is the URL for your WebEx site, followed by a forward slash (/) and the word "admin".
   Example: ***https://example.webex.com/admin***
2. On the left navigation bar under **Manage Site**, choose **Site Settings**. The **Site Settings** screen appears.
3. Scroll down to **OneTouch TelePresence Options**, as shown in the screenshot.

   Figure 30: Configuring Cisco WebEx Connection Settings



Site Settings for: Common

Select Common for settings that apply to more than one service
Select a service for settings that are specific to one service

OneTouch TelePresence Options

☑ Allow Cisco WebEx OneTouch meetings (MC only)

Enter the Cisco TMS (Cisco TelePresence Management Suite) booking service URL to connect your WebEx site to the TelePresence scheduling system.
Cisco TMS booking service URL: https://ctg-alpha-scheduler1.cisco.com (Example: https://tmsbookinghost.domain.com)

☑ List TelePresence meetings on calendar
☐ Send invitation email to meeting host
☑ Display toll-free number to participants
☑ Enable TelePresence bandwidth control
☐ Display TelePresence welcome screen

WebEx VoIP and video connection:
● Automatically encrypted UDP/TCP SSL
○ TCP SSL

☐ Disable Hybrid VoIP

4. Click to select **Allow Cisco WebEx OneTouch meetings (MC only)**.
   If not checked, Cisco WebEx will be disabled on this site and the rest of the Cisco TelePresence integration options will be grayed out.
5. If you are deploying the CMR Hybrid solution with the option to schedule meetings using the WebEx and TelePresence Integration to Microsoft Outlook, you must enter the host address for the TelePresence Management Suite Extension for Microsoft Exchange (TMSXE) in the **Cisco TMS booking service URL** field. (Example: *https://tmsxe.example.com*)
   For more information about configuring Cisco TMSXE, see Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange [p.118]

6. Click to select **List Cisco TelePresence meetings on calendar** so that scheduled meetings hosted by each user appear under **My WebEx Meetings** on their WebEx site.

Note: This option is removed in WebEx Meeting Center WBS29.13. TelePresence meetings will automatically appear in the list of meetings a user hosts on the WebEx site. TelePresence meetings a user is invited to are not displayed under **My WebEx Meetings**.

7. Click to select **Send invitation email to meeting host**. This allows the meeting information email to be sent to the Cisco WebEx host after the meeting is scheduled.
8. Click to select **Display toll-free number to attendees**. This enables the system to show the toll-free number that attendees can call to join the meeting.
9. (Optional) If you want to display the TelePresence welcome screen, click to select Display TelePresence welcome screen. The welcome screen displays the participants that are currently connected to the meeting as well as other meeting information. It is displayed when no content is being shared by participants. The welcome screen is off by default.
10. (TSP audio only) If deploying TSP audio, you may need to click to select **TSP identity code** and enter the code associated with your TSP (contact your TSP to determine if you need to do this, and which code you need to enter).
    Note: TSP Call-in User merge feature should already be configured and working in regular WebEx meetings before you set up CMR Hybrid on your site.
11. In the WebEx VOIP and video connection section, select a connection method between the WebEx meeting application and the multimedia server (VoIP and video):
    a. **Automatically encrypted UDP/TCP SSL**—(**Recommended**) Allows the WebEx meeting application to connect to the multimedia server by using encrypted UDP. If the UDP connection is not allowed, the application falls back to SSL. This is the most flexible option, particularly if you need to minimize traffic congestion between the WebEx application and your telepresence devices
    b. **TCP SSL**—Allows the WebEx meeting application to connect to the multimedia server by using SSL. **IMPORTANT: TCP/SSL SHOULD ONLY BE SELECTED BASED ON RECOMMENDATION FROM CISCO TAC. IN ALL OTHER CASES, UDP SHOULD BE SELECTED.**
12. (Optional) If you do not want users to use VoIP audio on this WebEx site, check the box **Disable Hybrid VOIP**.
    This disables VoIP for all meetings on the site, not only CMR Hybrid meetings.
13. Scroll to the bottom of the page and click **Save** to save your settings.

Proceed to Assigning the Meeting Center TelePresence Session Type [p.152] to complete your setup.

Assigning the Meeting Center TelePresence Session Type

You must assign the Meeting Center TelePresence session type to host accounts in the WebEx Site Administration interface to complete your setup. You can do so by either opening the Edit User screens for an individual user, or by selecting the appropriate session type for each user from the Edit User List screen. When you add a new user, this session type is assigned by default. Check for or configure this session type using the steps in the following sections:

- Adding the Cisco TelePresence Session Type in the List of Users [p.152]
- Adding the Cisco TelePresence Session Type in the Edit User Screen [p.154]

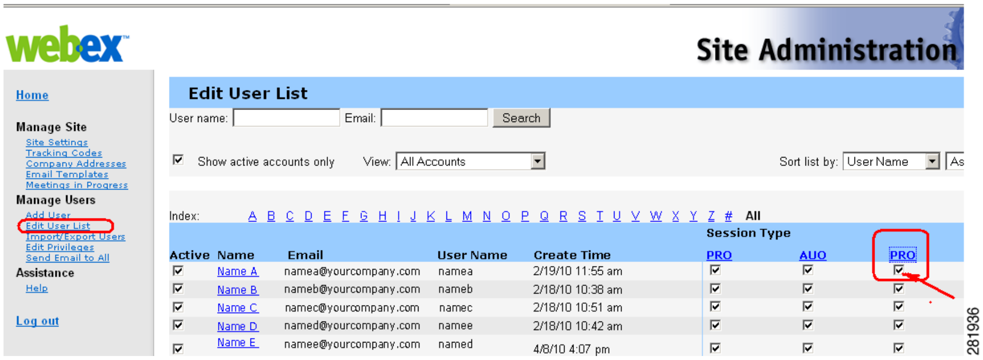
Support for Custom Session Types

With WebEx WBS29 or later, custom session types can be created which allow customers to restrict WebEx features for a specific group of users. For example, you could create a custom session type to disable recording, chat or annotation for a certain group of users. The Default TelePresence Session Type (which can be set to a custom session type) is used by default when a meeting organizer schedules a meeting. If the meeting organizer is scheduling the meeting using the WebEx and TelePresence Integration to Outlook plug-in, they will be able to select a different custom session type, if it has been configured at the Site Administration level. The WebEx site administrator can selectively decide which users have access to specific custom session types. When a meeting organizer schedules using Cisco TMS, Smart Scheduler or the WebEx Scheduling Mailbox, the Default TelePresence Session Type is always used. To enable custom session types for your WebEx site, contact WebEx cloud services. Once enabled, you can create a custom session type by going to the left navigation bar under **Session Types**, and choosing **Add Custom Type**. For details on how to create a custom session type, refer to the WebEx Site Administration help.

Adding the Cisco TelePresence Session Type in the List of Users

1. In the left navigation bar under **Manage Users**, choose **Edit User List**. The Edit User List screen appears, as shown in the screenshot.

   Figure 31: WebEx Site Administration - Edit User List



Edit User List

User name: Email:

☑ Show active accounts only View: All Accounts Sort list by: User Name As

					Session Type		
Active	Name	Email	User Name	Create Time	PRO	AUO	PRO
☑	Name A	namea@yourcompany.com	namea	2/19/10 11:55 am	☑	☑	☑
☑	Name B	nameb@yourcompany.com	nameb	2/18/10 10:38 am	☑	☑	☑
☑	Name C	namec@yourcompany.com	namec	2/18/10 10:51 am	☑	☑	☑
☑	Name D	named@yourcompany.com	namee	2/18/10 10:42 am	☑	☑	☑
☑	Name E	namee@yourcompany.com	named	4/8/10 4:07 pm	☑	☑	☑

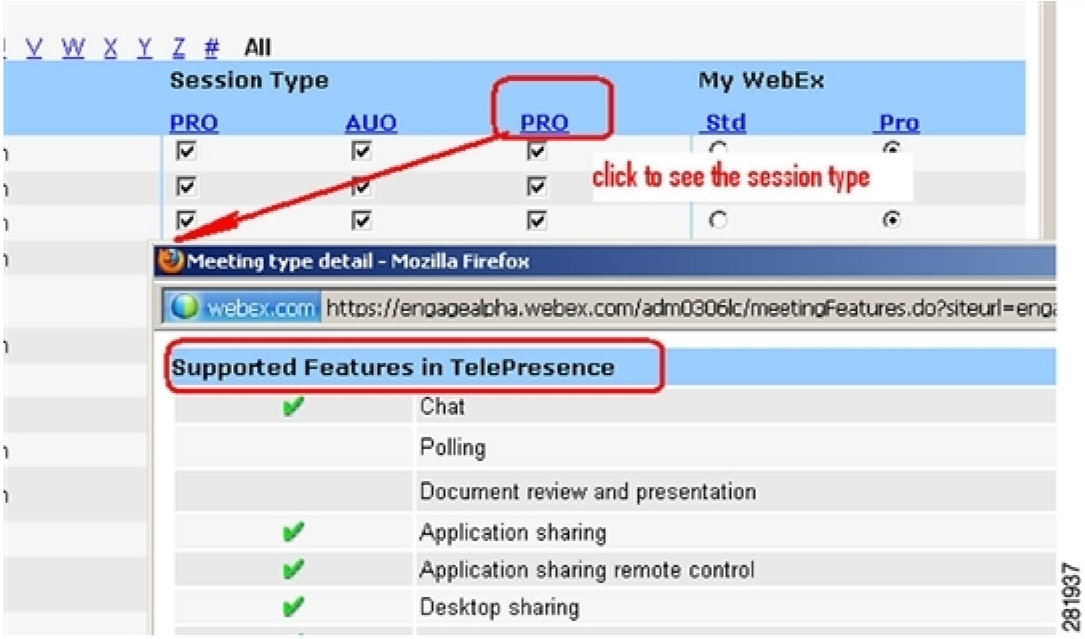
2. Identify which PRO column represents the Meeting Center TelePresence session type.

Each Cisco WebEx user account has a corresponding set of Session Type check boxes that indicate which Cisco WebEx session types have been enabled for that user; "Meeting Center TelePresence" is one of the "PRO" sessions types. (Other session types, such as Meeting Center Pro meeting, can also have a "PRO" headline, as shown in Assigning the Meeting Center TelePresence Session Type [p.152].) To determine which column represents the Meeting Center Telepresence session type, click any of the "PRO" Session Type headers. A separate window opens that describes that session type, as shown in Figure 32: Supported Features in TelePresence [p.153]. Locate the column that brings up the session type feature list titled "Supported Features in TelePresence"; this is the Meeting Center TelePresence session type.

Note: The number of session type columns is determined by how many session types the WebEx site supports.

3. To verify that a user is assigned the Meeting Center TelePresence session type, locate the user entry on the Edit User list and select the check box for the appropriate PRO session type identified in Step 2.
4. Scroll to the bottom of the page and click **Submit**.
   If you do not find the Meeting Center TelePresence session type, or if there is no "Supported Features in TelePresence" window present after you have clicked all "PRO" Session Types, the site is not properly configured for CMR Hybrid.

Figure 32: Supported Features in TelePresence



V W X Y Z # All
click to see the session type
Meeting type detail - Mozilla Firefox
webex.com
https://engagealpha.webex.com/adm0306lc/meetingFeatures.do?siteurl=eng
281937

Session Type PRO	AUO	PRO	My WebEx Std	Pro
☑	☑	☑	○	●
☑	☑	☑		
☑	☑	☑	○	●

	Supported Features in TelePresence
✓	Chat
	Polling
	Document review and presentation
✓	Application sharing
✓	Application sharing remote control
✓	Desktop sharing

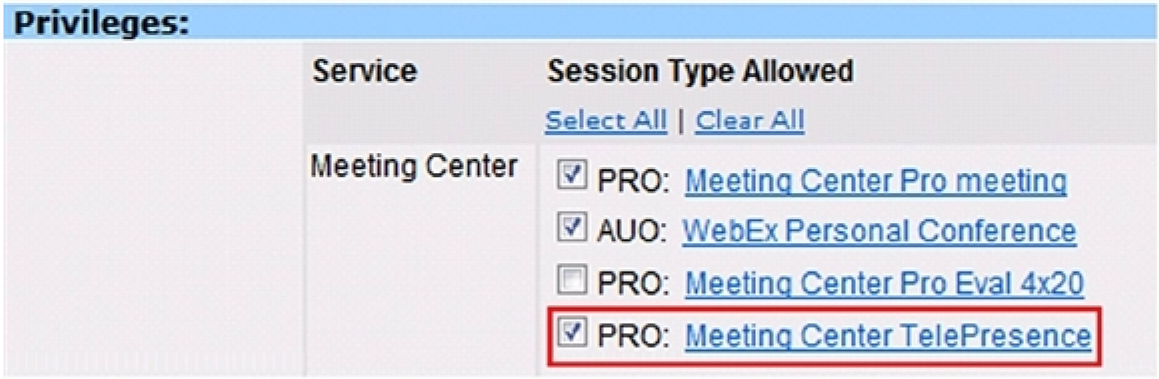
Note: This session type will be assigned by default when you create new host accounts by using the Add User link on a TelePresence-enabled WebEx site. The user must have this session type assigned in order to schedule CMR Hybrid meetings. If this site is an existing site updated to CMR Hybrid, you must add the Meeting Center TelePresence session type to existing users.

Adding the Cisco TelePresence Session Type in the Edit User Screen

You can also set the Meeting Center TelePresence session type in the account settings for each individual user. Do the following while still on the **Manage Users** > **Edit User List** page:

1. Locate the user entry and click on it to open the Edit User window for that account.
2. Scroll down to the Privileges section. The assigned session types are shown in the Session Type Allowed box, as shown below.

   Figure 33: Session Types Allowed

   Privileges:

Service	Session Type Allowed
	Select All | Clear All
Meeting Center	☑ PRO: Meeting Center Pro meeting ☑ AUO: WebEx Personal Conference □ PRO: Meeting Center Pro Eval 4x20 ☑ PRO: Meeting Center TelePresence

3. Required. Check the box for **PRO: Meeting Center TelePresence**, as shown circled in red in Assigning the Meeting Center TelePresence Session Type [p.152].
4. Click the **Update** button at the bottom of the window to save your **PRO: Meeting Center TelePresence** Session Type setting.

   This completes setting meeting center Cisco TelePresence Session Type privileges in the Cisco WebEx Site Administration. Your Cisco WebEx account is now fully integrated and provisioned.

Important: The TelePresence session type is enabled by default for all new users accounts, but it can be turned off, if desired.

Note: The functionality and appearance of the WebEx Productivity Tools integration to Microsoft Outlook changes when CMR Hybrid is enabled. See the WebEx and TelePresence Integration to Outlook User Guide available from your Meeting Center User Guides page for more information.

Network-Based Recording of CMR Hybrid Meetings

With release WBS29 of WebEx, meeting organizers can now record CMR Hybrid meetings.

- The WebEx and TelePresence Integration to Outlook and WebEx Meeting Center client automatically discover if recording is enabled and display the appropriate message.
- Playback of a recorded meeting displays both WebEx and TelePresence video with content share, chat and polling (if enabled).
- User can navigate through recording via playback controls or clicking thumbnails of the video.
- User can see a visual representation in the recording of when participants are talking.

Note: Network-based recording is enabled by WebEx Cloud Services.

Installing the WebEx and TelePresence Integration to Outlook

Meeting organizers who want to schedule meetings using the WebEx and TelePresence Integration to Outlook plug-in, must download and install the WebEx Productivity Tools with TelePresence from your WebEx site.

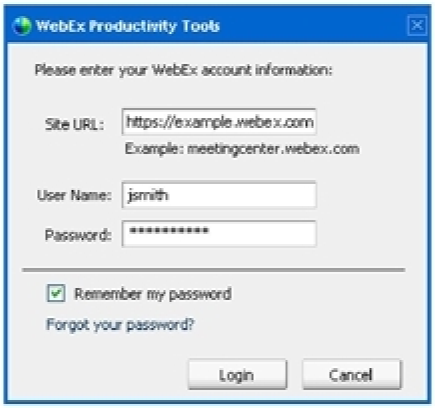
Before you install, make sure you have the following information for your WebEx site and TMSXE:

- WebEx Site URL
- WebEx User Name
- WebEx Password
- TMSXE User Name
- TMSXE Password

Note: Contact your WebEx or IT administrator for this information.

To install the WebEx Productivity Tools, users must do the following:

1. Open a browser and go your WebEx site.
2. Click **My WebEx**.
3. Log in to your account.
4. If your site is enabled to automatically prompt you to download the WebEx Productivity Tools, you will be presented with that option. If, so click **Yes** to begin the download and then skip to step 7. If not, go to the next step.
5. In the left-hand navigation bar, click **Productivity Tools Setup**.
6. The **ptools.msi** file is downloaded to your computer.
7. After the download is complete, open **ptools.msi** and follow the on-screen instructions to install the WebEx Productivity Tools.
8. During the installation you must log in to your WebEx site.
   WebEx Productivity Tools Login



WebEx Productivity Tools

Please enter your WebEx account information:

Site URL: https://example.webex.com

Example: meetingcenter.webex.com

User Name: jsmith

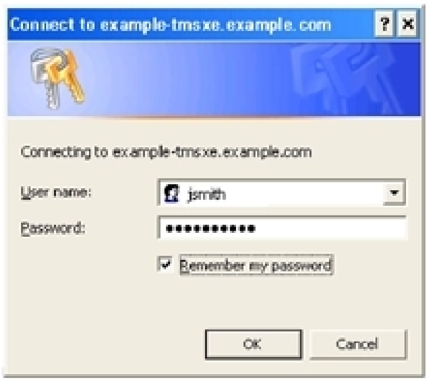
Password: ***********

☑ Remember my password

Forgot your password?

9. Enter your WebEx Site URL, User Name, Password and click **Login**.
10. After logging in, the WebEx Productivity Tools communicates with the server and then you are asked to

log into Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE).
Cisco TMSXE Login


Connect to example-tmsxe.example.com

Connecting to example-tmsxe.example.com

User name: jsmith

Password: ●●●●●●●●●●●

☑ Remember my password

11. Enter your TMSXE User name and Password and click **OK**.
12. When the message "WebEx Productivity Tools are installed" appears, click **OK**.
13. Close the Productivity Tools window.

You can now open Microsoft Outlook and schedule CMR Hybrid meetings using the WebEx and TelePresence Integration to Outlook.

Setting the Time Zone and Language Preferences for a User's WebEx Account

For best results, meeting organizers using Outlook for scheduling, should do the following:

- Set their WebEx and Outlook time zones to the same time zone.
  If a meeting organizer's WebEx and Outlook time zones do not match, meetings will not be scheduled at the same time in both WebEx and Outlook.
- Make sure their preferred language is selected in their WebEx account.
  The selected language is the language that all invitees will see in the meeting invitation.

To set the WebEx time zone and preferred language for a WebEx account, users must do the following:

1. Open a browser and go to your WebEx site.
2. Click **My WebEx**.
3. Enter your WebEx username and password and click **Log In**.
4. If you are presented with an option to download the WebEx Productivity Tools and you have already downloaded them, click **Later**. If you wish to download and install them now, refer to step 4 of Installing the WebEx and TelePresence Integration to Outlook [p.156]
   The My WebEx Meetings page appears.
5. In the right corner of the page, the current language and time zone settings are displayed.
6. To change the language and time zone, click on the link that displays either the current language or time zone.
7. The **Preferences** page appears.
8. Using the **Time zone** and **Language** menus, select the time zone and language you wish to use for your CMR Hybrid meetings.
9. Click **OK**.

Configuring TSP Audio for a User's WebEx Account

Meeting organizers who need to schedule CMR Hybrid meetings that use TSP audio must add TSP audio provider information to their account.

For details, refer to Configuring TSP Audio for CMR Hybrid [p.142].

Where to Go Next

For complete information about managing your Cisco WebEx Administration Site account, refer to the Help on your WebEx site.

Scheduling CMR Hybrid Meetings

First Published: June 23, 2014

This chapter provides a background on how to schedule CMR Hybrid meetings, with tips and known issues. It contains the following sections:

Introduction

This chapter provides an overview of how to schedule CMR Hybrid meetings using TMS and useful information, tips and known issues about CMR Hybrid meetings.

In addition to scheduling using TMS, there are up to 3 additional ways to schedule a CMR Hybrid meeting:

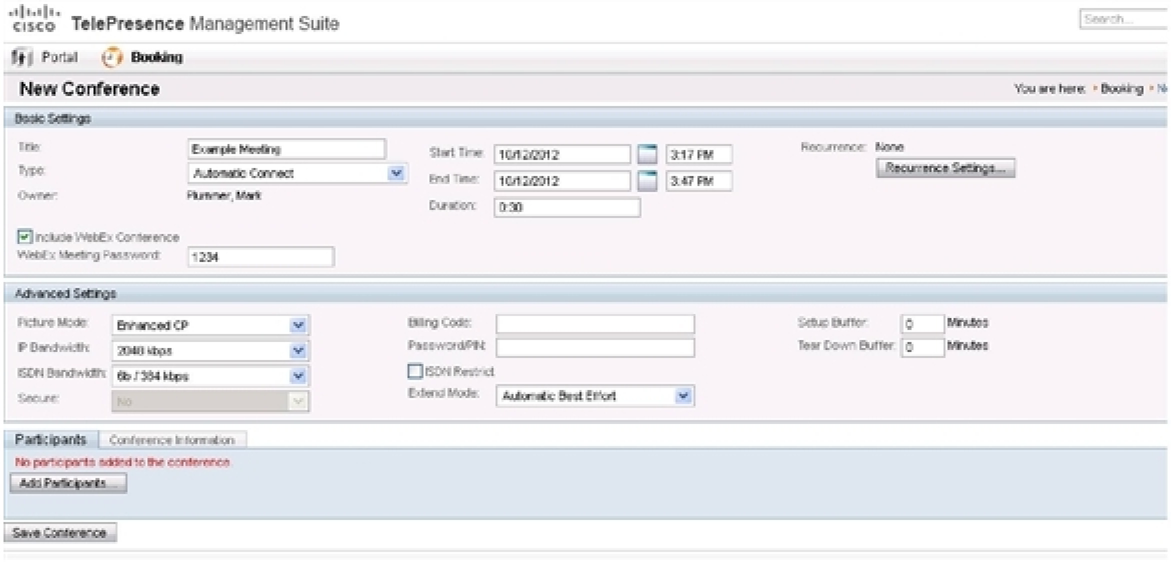
- Using the Cisco WebEx and TelePresence Integration to Outlook
  With the WebEx and TelePresence Integration to Outlook, users can schedule CMR Hybrid meetings directly from Microsoft Outlook for Windows or Mac. Advanced options like adding external video and audio dial-in participants are also available.
  For scheduling information, see WebEx and TelePresence Integration to Outlook Quick Reference Guide
  For additional information, including how to schedule a meeting on behalf of another person or to assign a delegate to schedule meetings for you, refer to the WebEx and TelePresence Integration to Outlook help available in Outlook or the user guide, available on your WebEx site.
- Using the Cisco Smart Scheduler
  With Cisco Smart Scheduler, Macintosh, mobile and other non-Windows users can schedule CMR Hybrid meetings using a simple web-based interface which is touch-screen friendly.
  For scheduling information, refer to the Cisco Smart Scheduler and WebEx Scheduling Mailbox Quick Reference Guide
  For additional information, including supported browsers and mobile platforms, refer to the Cisco TelePresence Management Suite Provisioning Extension (TMSPE) release notes.
- Using the Cisco WebEx Scheduling Mailbox
  With the Cisco WebEx Scheduling Mailbox, users without the WebEx and TelePresence Integration to Outlook can create a TelePresence Enabled WebEx meeting in Outlook by inviting TelePresence rooms and then adding WebEx to the meeting by including a special invitee; the WebEx Scheduling Mailbox. The mailbox may be called simply "webex" or something different. It as configured by the administrator and provided to users.
  For additional information, refer to the Cisco TelePresence Management Suite Extension for Microsoft Outlook (TMSXE) Installation Guide and release notes.
  For scheduling information, refer to the Cisco Smart Scheduler and WebEx Scheduling Mailbox Quick Reference Guide

Scheduling CMR Hybrid in Cisco TMS

When scheduling conferences with Cisco TMS, it is not necessary for the user to worry about network protocols, MCUs, or gateways. Cisco TMS handles infrastructure choices and compatibility checking of all these things automatically. Advanced users may still tune and tweak the selected methods for the conference as needed.

To schedule a CMR Hybrid Meeting:

1. Log in to Cisco TMS.
2. Go to **Booking** > **New Conference**.


cisco TelePresence Management Suite
Search...
Portal
Booking
You are here: • Booking • N

New Conference

Basic Settings

Title: Example Meeting
Type: Automatic Connect
Owner: Plummer, Mark
Start Time: 10/12/2012 3:17 PM
End Time: 10/12/2012 3:47 PM
Duration: 0:30
Recurrence: None
☑ Include WebEx Conference
WebEx Meeting Password: 1234

Advanced Settings

Picture Mode: Enhanced CP
IP Bandwidth: 2048 kbps
ISDN Bandwidth: 6b / 384 kbps
Secure: No
Billing Code:
Password/PIN:
□ ISDN Restrict
Extend Mode: Automatic Best Effort
Setup Buffer: 0 Minutes
Tear Down Buffer: 0 Minutes

Participants | Conference Information

No participants added to the conference

3. For Title, enter a conference title. It will be displayed in all Cisco TMS interfaces, and in email notifications about the meeting.
4. For Type, select either **Automatic Connect** or **One Button to Push**.
   - Automatic Connect: Cisco TMS automatically connects all participants at the meeting start time.
   - One Button to Push: Meeting dial-in information is automatically displayed on endpoints that support One Button to Push. Participants on those endpoints join the meeting by pressing a button. For endpoints that do not support One Button to Push, the meeting organizer adds a video dial-in number.

   Note: For information about additional types, refer to the TMS help.

5. Set the **Start Time** and the **End Time** or **Duration** for the meeting.
6. Make sure **Include WebEx Conference** is checked.
7. Optionally, enter a **WebEx Meeting Password**.

   Note: If you do not enter a password, WebEx will automatically generate one. It will be displayed on the Confirmation page, after you successfully schedule the meeting.

8. Optionally, click **Recurrence Settings** to create a series of meetings that are tied together, such as a weekly or daily meeting.

   Note: Advanced settings are optional. Most settings will take their default values from the Conference Default values configured under Administrative Tools. Refer to the help for an overview of all available settings. For details on the Advanced Settings, click the Help button in Cisco TMS

Note: If Secure is set to *Yes*, Cisco TMS will only allow systems that support encryption to participate in the conference.

9. Optionally, add notes about the meeting in Conference Information, which will appear in the meeting invitation.
10. In the Participant tab, click **Add Participant** and a new window will appear.
11. Available participants and a planner view with their availability is displayed based on existing scheduled and ad hoc meetings. The colored vertical lines represent your current requested time for the scheduled meeting.
12. Click the tabs to have participants listed by type. If you have used scheduling before, the default tab is Last Used with quick access to the systems you have used recently.
13. Hover over any system, or the blocks in the planner view, for additional detail about the system or scheduled meeting.
14. Add participants to the meeting by selecting their checkbox and clicking the **>** button to add them to the list of selected participants on the right side of the window. Adding network infrastructure components like MCUs and Gateways is optional as Cisco TMS will handle this for you automatically.
15. Use the External tab to add systems not managed by Cisco TMS, for example endpoints in other organizations, or telephone participants.
16. For dial-out participants, enter their contact information, and Cisco TMS will automatically connect them to the conference at the scheduled time.
17. For dial-in participants (including endpoints that do not support One-Button-to-Push), Cisco TMS will reserve the capacity needed to host the site in the conference and will provide you with precise dial-in information to forward to the participant.
18. When all participants have been added, click **OK**.
19. You are returned to the conference page, with the participant section of the page now showing your selected participants, and some additional tabs. These additional tabs allow advanced scheduling tasks such as altering how calls are connected, or setting specific MCU conference settings for the meeting.
20. Use the Video Conference Master drop-down list to determine which system should be considered the meeting organizer. Not all telepresence systems support the necessary features for this functionality, and only systems that are eligible will be displayed in this list. This is the system that will be prompted:
    - to connect the conference if it is not scheduled for automated call launch.
    - to extend the conference when it is about to expire.
21. Click **Save Conference**. When the conference is saved, Cisco TMS will do all the routing calculations to determine the best way to connect your selected participants.
    - If Cisco TMS is able to complete your request:
        - You are presented with a confirmation page indicating that your conference has been saved and showing the details of your meeting, including the participant list and listing how each of those participants are scheduled to connect to the conference and the exact dial string any participants must dial.
        - You will also receive an email confirmation from Cisco TMS with all meeting information, including WebEx and video dial-in information, and an ICS attachment for saving the event in your Outlook (or a compatible) calendar. Open the ICS attachment and save it to your calendar.
        - If your WebEx site is set up to send email confirmations, you will receive two additional email notifications from WebEx: 1. An email with the subject line "Meeting Scheduled" which contains the host key and the WebEx information for the meeting 2. An email with the subject line "(Forward to attendees) Meeting Invitation" which contains only the WebEx information for attendees.

- If Cisco TMS is unable to complete your booking request:
  1. You are returned to the New Conference page. A message banner states why it was not possible to save the meeting. This may be due to lack of availability, lack of network resources, or no known route to connect the participants together.
  2. Edit the conference settings to try to resolve the issue and try saving the conference again.
  3. After successfully scheduling your meeting, invite people to the meeting using your calendar application.

For information about the CMR Hybrid meeting experience, see CMR Hybrid Experience [p.19].

Information, Tips and Known Issues About CMR Hybrid Meetings

The following section contains useful information, including tips and known issues relating to CMR Hybrid meetings. The information is divided into sections corresponding to each product that is part of the CMR HybridSolution.

Cisco TMS

- Cisco TMS can be configured so that meetings must be approved by the Cisco TMS administrator before getting booked. This feature can be used to regulate port usage at companies that want to limit / regulate usage.
- Cisco TMS limits the number of ports to the number selected under the external tab of the Cisco TMS meeting when it is scheduled.
- Extending a meeting is supported for both TelePresence and WebEx using the Extend Mode setting when scheduling a meeting. Meeting extension is not guaranteed. If resources (ports) are fully booked at the scheduled end time of the meeting, the meeting will end.
- A meeting organizer scheduling a meeting using the WebEx and TelePresence Integration to Outlook, should never modify that meeting later in Cisco TMS.
  If the original meeting is modified later in Cisco TMS, the meeting information in Cisco TMS will fall out of sync with the meeting organizer's Outlook calendar. The reason for this is that Cisco TMSXE does not have write access to the meeting organizer's calendar and, as a result, can't make any changes to it.

MCU and TelePresence Server

- At the start of the meeting, the MCU/TelePresence Server calls into WebEx, even if there are no TelePresence or WebEx participants.
- The MCU/TelePresence Server's role is different from a regular WebEx participant. When joining the meeting, if there is no meeting host currently in the meeting, the MCU becomes the default host and starts the meeting.
- If there is already a WebEx host, MCU/TelePresence Server will not become the host.
- If WebEx host leaves the meeting, the MCU/TelePresence Server becomes the host and the meeting continues.
- If MCU/TelePresence Server leaves the meeting before the WebEx host leaves, the meeting continues.
- If MCU/TelePresence Server leaves the meeting after the WebEx host leaves, the meeting ends.
- If WebEx host leaves the meeting after the MCU/TelePresence Server leaves, the meeting ends.
- If WebEx host stays in the meeting after the MCU/TelePresence Server leaves, the WebEx meeting continues.
- TelePresence Server by default, sends video in the ActivePresence screen layout, which displays the active speaker in a full screen pane with additional participants appearing in up to six equally sized overlaid panes at the bottom of the screen (up to four panes for 2 and 4 screen endpoints). In full-screen mode in WebEx, WebEx participants appear in equally sized panes below the TelePresence video at the bottom of the window. MCU by default, sends video in a full-screen layout.

Endpoints

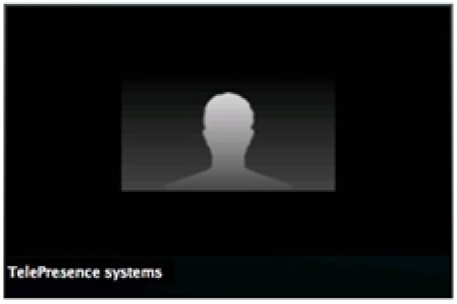
- Participants joining the meeting from any TelePresence endpoint may not see the presentation from WebEx if they are using their endpoint as a computer monitor.
- Content presented from an EX60 can take a long time to appear. If the endpoint is registered to Unified CM, this can be resolved by enabling User-Agent passthrough in Unified CM.

Cisco TMSXE

When booking a meeting using Web Scheduling Mailbox, if TMSXE detects an error condition (ex: not able to connect with WebEx server), the error email is sent in plain text format to the meeting organizer.

WebEx

- If a WebEx participant's camera is not on, the participant displays as a black silhouette.
- In the WebEx Meeting Center, all TelePresence endpoints are displayed as one WebEx participant called "TelePresence systems" both in the Participant list and when a TelePresence user is the active speaker.
- In the Meeting Center full screen view, the "TelePresence systems" participant appears as a black silhouette, as shown below.
  "TelePresence systems" in Full Screen View



- The WebEx host can mute all or individual participants after they join the meeting. It is not possible to mute TelePresence participants through the WebEx client. TelePresence participants must mute themselves.
- To mute WebEx participants, you have to be the WebEx host.
  To reclaim the host role, you have to get the WebEx host key.
- The meeting is started by the first participant who joins the meeting (host or other WebEx participant). The rest of the participants "join" the meeting.
- A non-host participant can start a meeting only if the "Join Before Host" feature is enabled on the site, and its start time could be 5/10/15 minutes (set a time of scheduling) before the scheduled time. Otherwise, the participant must wait for the meeting to be started by the host before they can join.
- If a WebEx audio only participant is talking, the last video participant to talk is displayed until the next video participant speaks.
- The user's Outlook time zone and WebEx account time zone must be the same for the meeting to be scheduled at the correct time in both Outlook and WebEx.
- When the WebEx portion of the meeting ends, the audio will end too.
- When the WebEx host leaves the meeting, a message appears asking them if they want to leave the meeting without ending it for all participants. They can choose to leave or end the meeting.

- The link bandwidth between the MCU and WebEx is set by the WebEx client with the lowest bandwidth. The bandwidth can go up as soon as the WebEx client with the poorest bandwidth leaves the meeting. For example, if a WebEx client that joins the meeting is only capable of 360p, the maximum bandwidth from telepresence to all WebEx participants will be 360p. When that participant leaves the meeting, if all other clients are capable of a higher bandwidth, like 720p, the bandwidth will go up for all WebEx participants.

Troubleshooting

First Published: June 23, 2014

This chapter describes troubleshooting tips and information. It contains the following sections:

Verifying and Testing

Cisco WebEx Site Administration Online Help

For complete information about using Cisco WebEx Site Administration, go to the Cisco WebEx Site Administration Help:

1. Log in to Site Administration for your WebEx site.
   This is the URL for your WebEx site, followed by a forward slash (/) and the word "admin".
   Example—*https://example.webex.com/admin*
2. In the left-hand side of page under Assistance, click the **Help** link.

Troubleshooting Tips

This section provides troubleshooting tips for problems with the following aspects of a CMR Hybrid meeting:

- Problems with Scheduling a Meeting [p.171]
- Problems with Starting or Joining a Meeting [p.173]
- Problems During a Meeting [p.174]
- Problems with a TSP Audio Meeting [p.179]
- Problems with TelePresence Server and MCU [p.181]
- CMR Hybrid_WebEx_Site_Administration_Settings_Differences_Between_WBS28.12.27_Lockdown_Version_and_WBS29.13.x_Lockdown_Version
- Known Issues/Limitations with WebEx Site Administration WBS29.x for CMR Hybrid [p.184]

Problems with Scheduling a Meeting

This section describes possible issues the meeting organizer may experience when scheduling a meeting using Cisco TMS.

See the table for troubleshooting information on how to solve common problems that prevent meetings from being scheduled correctly.

Table 19: Problems with Scheduling Meetings

Problem or Message	Possible Causes	Recommended Action
The meeting organizer receives no email from Cisco TMS to confirm the meeting is scheduled.	Cisco TMS configure to send confirmation email.	Check Cisco TMS configuration. If Cisco TMS configuration is correct, check antivirus/firewall program(s) to see if they are blocking the Cisco TMS from sending.
After meeting organizer schedules a meeting using TMS, the following error is displayed: "An unexpected error occurred while communicating with WebEx." The meeting is created, but there are problems with the WebEx configuration. They receive a meeting confirmation email that contains no WebEx information.	Meeting organizer's WebEx host account is not provisioned with the Meeting Center TelePresence session type.	Log into WebEx Site Administration for your WebEx site and make sure the meeting organizer's host account has the Meeting Center TelePresence session type enabled. For more information, refer to: Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account [p.150].

Table 19: Problems with Scheduling Meetings (continued)

Problem or Message	Possible Causes	Recommended Action
Meeting is not listed on the endpoint display.	More than one scheduling server is managing the endpoint (Example: Cisco TMS and CTS-Manager and at the same time). Other causes: ▪ Scheduled meeting type is not One-Button-to-Push (OBTP). Only OBTP meetings appear on an endpoint. ▪ Network connection failure between endpoint and Cisco TMS.	If pushed to all but one endpoint, then check the network connection. If not pushed to any endpoints, check to see if Cisco TMS is down. In Administrative Tools > Configuration > WebEx Settings, select the WebEx site and make sure Connection Status is "Connection OK".
WebEx scheduling error in Cisco TMS (when clicking Save) **Symptom**: Cisco TMS displays 'Unable to include WebEx conference. Incorrect WebEx username or password.'	Network problems with WebEx site. WebEx user doesn't exist on WebEx site. **Cause**: WebEx site configured for this organizer does not recognize the WebEx username/password configure for the meeting organizer.	Check WebEx account user profile. **Recommended Action**: Check the WebEx Username/Password for the WebEx site in the user personal information page. Or the WebEx site user credential information may have changed. In this case, check with WebEx site administrator. Refer to Cisco TMS Troubleshooting information. This issue is not limited to Cisco CMR Hybrid.
No confirmation emails from WebEx	Email is not enabled on the WebEx site	Check the WebEx site administrator.
Meeting is booked on the TMS but the WebEx does not exist.	Endpoints booked for the meeting are configured as mailboxes in Exchange but are not set to AutoAccept invitations.	Ensure that all endpoints that are available as mailboxes for booking in a Cisco CMR Hybrid meeting are set to AutoAccept in Exchange.
"We've hit a glitch in connecting to the telepresence scheduling system. Try again later."	TMSXE	Contact the TMSXE administrator.

Table 19: Problems with Scheduling Meetings (continued)

Problem or Message	Possible Causes	Recommended Action
I do not see the WebEx option when scheduling a meeting in TMS.	Your WebEx Username and Password have not been added to your TMS user profile.	Edit your TMS user and enter your WebEx username and password and then save. The WebEx option should now appear in the TMS scheduling UI.

Problems with Starting or Joining a Meeting

This section describes possible issues meeting participants may experience when starting or joining a meeting.

Refer to troubleshooting information in the table on how to solve common problems that prevent participants from starting or joining meetings.

Table 20: Problems with Starting or Joining Meetings

Problem or Message	Possible Causes	Recommended Action
Can't join the WebEx meeting	Meeting hasn't started yet	wait for meeting to start
No endpoint can join the TelePresence meeting.	TelePresence meeting doesn't exist. Call failed to be routed correctly.	1. Check MCU/TelePresence Server to make sure conference was created. 2. Check MCU/TelePresence Server event log. 3. Check VCS search history.
Single TelePresence participant can't join the meeting	Not enough video and audio ports. Call routing issue for the endpoint to MCU or TelePresence Server	Check event log for the meeting. Also check meetings in TelePresence Server or MCU. Administrator can lift the limit by changing the port value from the TelePresence Server Conferences page.
TelePresence participant can only join via audio only.	Not enough video ports are available.	Increase the video ports in Cisco TMS, TelePresence Server or MCU.
No TelePresence participants can join the meeting	Meeting has not started yet. Cisco TMS scheduled meeting does not support early start. Endpoint must wait until meeting has started to dial in. Total audio and video ports for the MCU/TelePresence Server have been used up. Another cause is that the port video/audio limit for the meeting has been reached.	If total port capacity of MCU/TelePresence Server has been reached, no action is required. For the case of the meeting limit being reached, the administrator can lift the limit from the TelePresence Server Conferences page.

Table 20: Problems with Starting or Joining Meetings (continued)

Problem or Message	Possible Causes	Recommended Action
MCU/TelePresence server disconnects after WebEx host joins the meeting.	WebEx host is currently joined to another meeting of which they are also the host.	Do not use the same WebEx host ID to join multiple meetings at the same time. Only one CMR Hybrid meeting can be run per host at a time.
I do not see a CMR Hybrid meeting I was invited to under **My WebEx Meetings** on my WebEx site.	CMR Hybrid meetings a user is invited to are not displayed under **My WebEx Meetings**.	None. Only CMR Hybrid meetings that a user hosts are displayed under **My WebEx Meetings**.

Problems During a Meeting

This section describes possible issues meeting participants may experience during a meeting.

Refer to troubleshooting information in the table on how to solve common problems during the meeting.

Table 21: Problems During the Meeting

Problem or Message	Possible Causes	Recommended Action
No WebEx welcome screen	Content disabled on MCU. Video call from MCU/TelePresence Server to WebEx failed. Call failure occurs for several reasons: ■ WebEx SIP dialing fails to reach destination due to unresolvable SIP URI ■ WebEx server(s) down ■ Issues with search rules in VCS ■ Media Encryption setting in VCS	■ Check MCU configuration and conference status. ■ Verify search rules to ensure that SIP URI being routed correctly to WebEx site. ■ Verify encryption setting in VCS for this zone. ■ If failure persists after above actions are taken, contact WebEx site administrator.

Table 21: Problems During the Meeting (continued)

Problem or Message	Possible Causes	Recommended Action
TelePresence is not linked to WebEx	Video call from MCU/TelePresence Server to WebEx failed. Call failure occurs for several reasons: ■ WebEx SIP dialing fails to reach destination due to unresolvable SIP URI ■ WebEx server(s) down ■ Issues with search rules in VCS ■ Media Encryption setting in VCS	-
Don't see video on WebEx	WebEx participant does not enable video. WebEx participant has a problem with their camera.	■ Make sure TelePresence and WebEx calls are connected. ■ Check to see if participants who joined TelePresence are sending video.

Table 21: Problems During the Meeting (continued)

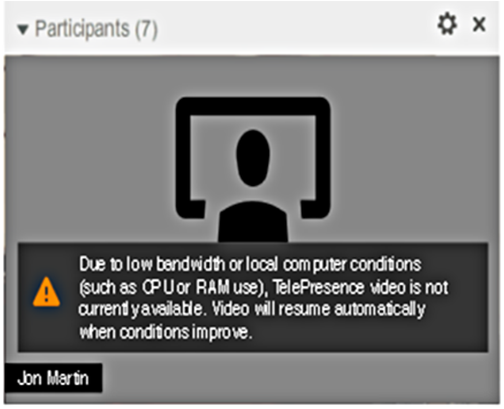
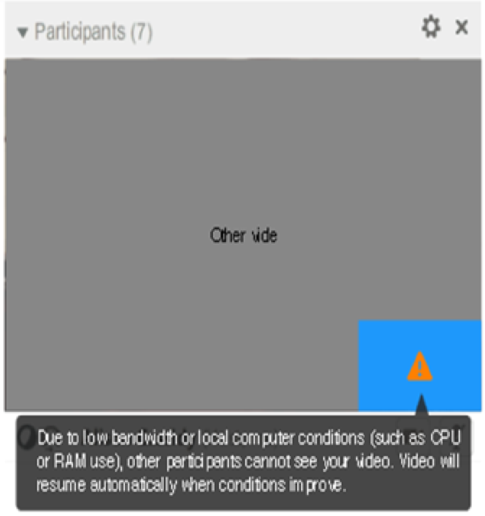
Problem or Message	Possible Causes	Recommended Action
Low-bandwidth warning in WebEx Meeting Center client on Windows or Mac: **Receiving from TelePresence**  Due to low bandwidth or local computer conditions (such as CPU or RAM use), TelePresence video is not currently available. Video will resume automatically when conditions improve. "Due to low bandwidth or local computer conditions, TelePresence video is not currently available." **Sending to TelePresence:**  Due to low bandwidth or local computer conditions (such as CPU or RAM use), other participants cannot see your video. Video will resume automatically when conditions improve.	■ Not enough bandwidth is available for the WebEx Meeting Center client. ■ The downspeed drops below 180p video resolution.	■ Meeting Center client will automatically retest with a lowered threshold (1.3 Mbps) for TelePresence to send to WebEx and will display video when conditions improve. ■ Verify there is enough bandwidth for the WebEx Meeting Center client. • 1.3 Mbps of sustained throughput is required to avoid the low-bandwidth warning where datasharing is active. ■ Disconnect and reconnect to the meeting to rejoin the main video. ■ Review Causes of Low Bandwidth Warning with WebEx Meeting Center Client on Windows or Mac [p.178] and Tips for Troubleshooting Low Bandwidth with the WebEx Meeting Center Client on Windows or Mac [p.179] ■ For details on Meeting Center client requirements for CMR Hybrid refer to: Prerequisites [p.10] ■ Before contacting support, get the audio and video statistics from the meeting. In the Meeting Center client during the meeting: • Select **Meeting > Audio & Video Statistics...** • or in Full-Screen view, right-click the active speaker's video and select **Audio & Video Statistics...**
Don't see video on TelePresence	-	■ Check to see if WebEx users have joined and are sending video.

Table 21: Problems During the Meeting (continued)

Problem or Message	Possible Causes	Recommended Action
Don't hear audio on WebEx	-	■ Check TelePresence call statistics and make sure TelePresence endpoint is not muted. ■ Check to see if WebEx users can hear each other.
Don't hear audio on TelePresence	-	■ Check TelePresence statistics to see if audio is being received from the WebEx side. In PSTN/TSP audio case check that the audio call is connected.
Don't see presentation shared from WebEx side on TelePresence side	-	■ Check TelePresence statistic for content channel status. ■ Check to see if WebEx users can see content from each other.
Don't see presentation from TelePresence side on WebEx side	-	■ Check TelePresence statistic for content channel status. ■ Check to see if WebEx users can see content from each other.
Don't see presentation from WebEx on WebEx side	-	■ Contact the WebEx administrator for assistance.
Don't see presentation from TelePresence side on TelePresence side	-	■ Check TelePresence call statistics to see if content channel is established. ■ Try to stop the restart sending content.
Presentation is displayed in main video	-	■ Check current call statistics for content channel. ■ Check to see if the SIP call encrypted.
Poor quality video from WebEx participants on TelePresence side	-	■ Check network bandwidth for possible poor network connection.
Poor quality video from TelePresence participants on WebEx side	Poor network connection	■ Check call statistics for TelePresence participants.
Audio skewed from video (lip sync issues)	In the case of PSTN/TSP audio, lip sync cannot be guaranteed	-

Table 21: Problems During the Meeting (continued)

Problem or Message	Possible Causes	Recommended Action
Active speaker does not switch in	-	■ Make sure audio and video calls are linked in PSTN/TSP case.
Video for active speaker call-in participant does not switch in when they speak and no phone icon associated with them.	1. WebEx site administrator not configured properly. 2. Audio call failed. 3. If the MCU sends the wrong participant ID.	■ Check in Cisco TMS CCC or on MCU to see if audio call failed. ■ Call-in user merge requires the site to have 'TSP identity code' enabled in WebEx site administrator. If disabled, call-in merge will not work even if you dial the correct value, and #1 is correct for InterCall.
Poor quality presentation from TelePresence participants on WebEx side	Possible network issue.	■ Check the bandwidth between TelePresence and WebEx.
Video from a WebEx participant frozen	Possible network issue.	■ Check the bandwidth between TelePresence and WebEx.
Meeting ends unexpectedly	-	■ Check TelePresence log to see any cause for the call drop.
Meeting didn't automatically extend	TelePresence is booked for another meeting starting at the end of the current one.	■ Check Cisco TMS booking list to confirm.

Causes of Low Bandwidth Warning with WebEx Meeting Center Client on Windows or Mac

Symptom 1: One Low Bandwidth warning when receiving TelePresence video in WebEx:

- UDP vs TCP (Fw ports, WebEx site settings)
- Other Applications running: Big emails, VPN clients, Virtualization sessions
- Wi-fi vs wired LAN access
- <400-500kpbs out to Internet

Note: Display of “low bandwidth” error messages (and content of message) differs between mobile WebEx clients and desktop clients.

Symptom 2: Everyone on WebEx receives a Low bandwidth warning when receiving TelePresence video in WebEx, or whenever sending WebEx video to TelePresence.

- Network conditions on the cascade link between WebEx and TelePresence (TS/MCU) have degraded.

Symptom 3: Certain WebEx clients with video on appear as just an avatar in TelePresence, when sending video to TelePresence.

- Same conditions as symptom 1 above.

Note: WebEx- clients (90p) video may still be seen. In that case, one WebEx active speaker may be visible in WebEx, but not in TelePresence, at the same time.

Symptom 4: No TelePresence Systems view in thumbnails (avatar only).

- This is by design, for consistency of experience with WebEx video (also, no ActivePresence thumbnails appear in the WebEx client when a TelePresence participant is the active speaker)

Tips for Troubleshooting Low Bandwidth with the WebEx Meeting Center Client on Windows or Mac

To troubleshoot low bandwidth with the WebEx Meeting Center client, do the following:

1. Review the WebEx Latency Troubleshooting Tips at: http://kb.webex.com/WBX28297
2. Ensure you have allowed **all** specified WebEx ports for your proxy and firewall. For detailed information, refer to How Do I Allow WebEx Traffic on My Network? at: https://kb.webex.com/WBX264
3. Ensure your VCS-Expressway or Expressway-E has the correct ports enabled, by reviewing Appendix 3: Firewall and NAT settings in: VCS Basic Configuration (Control with Expressway) x8.2 Deployment Guide
4. Review the TMS setting for WebEx participant bandwidth, by doing the following in TMS:
   a. Go to: **Administrative Tools** > **Configuration** > **WebEx Settings**
   b. Under WebEx Sites, click your WebEx site.
   c. On the WebEx Site Configuration page, make sure **WebEx Participant Bandwidth** is set to **2048 kbps** or higher.
5. Review the site administration settings for your WebEx site, by doing the following:
   a. Log in to WebEx Site Administration for your WebEx site.
   b. Under Manage Site in the left-hand navigation, click **Site Settings**
   c. Under WebEx VOIP and Video Connection, select **Automatically encrypted UDP/TCP SSL** to allow the Cisco TMS to connect over UDP with the TelePresence Gateway. If the UDP connection is not allowed, Cisco TMS will fall back to TCP.
   d. Under Site Settings, click **Cloud Collaboration Meeting Room Options**.
   e. Check **Enable video device bandwidth control**.
   f. On the Site Settings page, using the **Site Settings for** menu, select **Common**.
   g. Under Site Options, set the maximum video bandwidth allows the site administrator to set the maximum frame rate for video in a meeting. The default is 15 fps.

Problems with a TSP Audio Meeting

This section describes possible issues with a meeting that uses TSP audio.

Refer to troubleshooting information in the table on how to solve common problems with TSP audio meetings.

Table 22: Problems with a TSP Meeting

Problem or Message	Possible Causes	Recommended Action
TelePresence joins audio of host's previously scheduled meeting that had run beyond the scheduled end time.	The TelePresence system will dial into the hosts audio conference at the scheduled time. It is possible that the host is in a previous audio conference that is running overtime. Example: The host account used by TelePresence is that of a real WebEx host. If that host account has scheduled two back to back meetings (first one is WebEx meeting and the second one is TP+WebEx). Host starts first meeting and it runs overtime. But at the start time of the TelePresence+WebEx meeting, TelePresence dials into the TSP conference using the dumb-dial string, and may get into the conference. Result: TelePresence attendees hear the audio of the previous meeting. This may be a pretty well understood circumstance for customers due to the way TSP Audio works.	■ Have TelePresence recite audio prompt after joining the TSP audio. "Cisco Telepresence is now in the audio conference" (or similar). **Note:** Using API method does not resolve this.
TelePresence joins audio of host's previously scheduled meeting where the host had exited with the "keep audio conference running" option.	Similar to the above scenario - the host may have left the first meeting but used the "keep audio conference open" choice. Thus, as the audio conference of the first meeting continues, TelePresence eventually dials in. This may be a pretty well understood circumstance for customers due to the way TSP Audio works.	■ Have TelePresence recite audio prompt after joining the TSP audio. "Cisco Telepresence is now in the audio conference" (or similar). **Note:** Using API method does not resolve this.
"Host private conference code" can break DTMF dumb dial entry method in some cases (dial in as host + host has already dialed in).	If the TSP has implemented a "host private conference code" (where the host uses a conference code that is not the same as the one used by the attendees, thus avoiding the need for the host to enter a PIN number), the audio prompt call flow might break the dumb-dial of the MCU if the host has already dialed into the conference. (in our testing, this is when we heard all the foreign language prompts from the TSP bridge - it was the bridge barking about the fact that the host conf code is already in use).	■ Use API method....or... ■ Advice to TSP partners: If using a "hosts' private conference code", then consider allowing the TSP audio bridge to tolerate a second user dialing in using the host private conference code.

Table 22: Problems with a TSP Meeting (continued)

Problem or Message	Possible Causes	Recommended Action
Dial sequence cannot be issued on the fly via TSP API (unlike NBR).	The dial sequence for OT 2.0 integration with TSPs is only statically configurable in the Telephony Domain of site. This restricts a TSP somewhat, in case they might have different audio bridge infrastructures, different dial in numbers, etc. NBR, by contrast, allows for the static configuration as well as a dynamic configuration. The dynamic configuration is done by having the partner TSP Adapter send WebEx the NBR dial string at the time of meeting start via A2W_ RspCreateConference[NBRPhoneNumber].	■ Change the MCU logic, so that it starts the WebEx meeting and then collects the dial in string from WebEx at that time. The sequence will allow for WebEx to collect the dial string dynamically from the TSP as follows: a. TelePresence starts TelePresence meeting. b. TelePresence starts WebEx meeting. c. WebEx sends W2A_ CreateConference to TSP. d. TSP sends A2W_ RspCreateConference to WebEx (this would contain the TP dial string). e. WebEx sends dial string to MCU. f. MCU dials into the TSP bridge. The TSP API and TSP Server would need to change (among other components, of course).
The TSP Audio account info, used by the MCU dial string, is obsolete.	Since the MCU collects and stores the TSP dial string at the time of meeting schedule, to be used at the time of meeting start (which can be many weeks later), there is a possibility that the dial string will be obsolete and hence the call into the TSP conference will fail. This will happen if the default (first) TSP Audio account is changed during the time between TelePresence meeting schedule and TelePresence meeting start.	■ The above suggestion will solve this problem (making the TelePresence equipment collect the TelePresence dial string from WebEx at the time of meeting start, instead of at the time of meeting schedule.

Problems with TelePresence Server and MCU

This section describes possible issues with a meeting caused by TelePresence Server and MCU.

Refer to troubleshooting information in the table on how to solve common problems with TelePresence Server and MCU.

Table 23: Problems with TelePresence Server and MCU

Problem or Message	Possible Causes	Recommended Action
MCU/TelePresence Server disconnects shortly after connecting to WebEx. A SIP Bye message is received from the WebEx cloud.	WebEx host joins a meeting while already joined to a meeting of which they are also the host.	■ Do not use the same WebEx host ID to join multiple meetings at the same time. **Note:** Only one CMR Hybrid meeting can be run per host at a time.

CMR Hybrid WebEx Site Administration Settings Differences Between WBS28.12.27 Lockdown Version and WBS29.13.x Lockdown Version

Option	WBS28.12.27 lockdown version (WebEx OneTouch 1.0)	WBS29.13.x lockdown version (CMR Hybrid)
Enable CMR Hybrid - label change only	"Allow OneTouch TelePresence (MC only)"	"Allow Cisco WebEx OneTouch meetings (MC only)"
Connecting Cisco TelePresence to WebEx	Enter Cisco TelePresence Manager (CTSMAN) access code	Enter Cisco TelePresence Management Suite (TMS) booking service URL
List TelePresence meetings on calendar option	Available	Option removed. TelePresence meetings will automatically appear in host's meeting list.
Allow video options ■ TelePresence video ■ WebEx video	Available	Option removed. TelePresence video and WebEx video are always available when CMR Hybrid is enabled.
Welcome screen option	"Do not display host key in welcome screen"—This option is off by default. The Welcome screen always displays, but you can check this option to hide the meeting host key.	"Display TelePresence welcome screen"—The Welcome screen displays only when option is enabled. This option is unchecked by default. If you do check this option to display the TelePresence Welcome screen, the meeting host key will always display in that screen.
Allowing connections to CTMS systems options	Available	Option removed. CTMS is no longer supported in CMR Hybrid.
Disable Remote Control in desktop, application, and web browser sharing option	Available	Option removed. Custom session types allow you to restrict selected WebEx features from being available for your meetings.

Option	WBS28.12.27 lockdown version (WebEx OneTouch 1.0)	WBS29.13.x lockdown version (CMR Hybrid)
Disable Chat option	Available	Option removed. Custom session types allow you to restrict selected WebEx features from being available for your meetings.
Enable TelePresence bandwidth control option	Not Available	Option added. Enable to provide the best experience for all users during sharing or when video is shown in a CMR Hybrid meeting (ON by default).
Disable Hybrid VoIP	Not Available	Option added. Allows you to prevent users from connecting to WebEx audio through their computers. For example, you may choose to disable this option when your site is provisioned for TSP audio.

Note: Starting with CMR Hybrid, you can create custom session types, which allow you to restrict selected WebEx features.

Known Issues/Limitations with WebEx Site Administration WBS29.x for CMR Hybrid

To reduce the possibility of bandwidth issues for video, site administrators should make sure the following site administration options are set for CMR Hybrid users:

- Make sure that for **WebEx VoIP and video connection**, the **Automatically encrypted UDP/TCP SSL** option is always selected.
- Select **Site Settings** > **Site Options** and check the maximum video bandwidth option. This sets the maximum video frame rate for in-meeting video. The default setting is 15 fps.
- Under "OneTouch TelePresence Options," make sure **Enable TelePresence bandwidth control** is checked unless WebEx Support recommends altering it.
- Under "Meeting Options," make sure that **Turn on high-definition video** is turned on so that resolutions higher than 360p can be sent.

Site administrators should also make sure that the Meeting Center PRO TelePresence session type is enabled for your site:

- The **Meeting Center PRO TelePresence** session type will give users a different user interface in the WebEx Productivity Tools integration to Microsoft Outlook than the standard WebEx integration with Outlook.
- If you want existing users on your site to use CMR Hybrid, you need to batch-enable them for the **Meeting Center Pro TelePresence** session type—it is not enabled for them automatically.
- When your site is enabled for CMR Hybrid, the **Default for New Users** checkbox is automatically checked next to the **Meeting Center PRO TelePresence** session type site administration option. If you do not want new users to be enabled for CMR Hybrid automatically, you should uncheck the **Default for New Users** checkbox.
- You can also create additional custom session types based on the Meeting Center TelePresence session type.

Site administrators cannot make any changes to CMR Hybrid user interface for WebEx Productivity Tools. For example, administrators cannot change the branding for the CMR Hybrid Meeting Options panel within the Outlook integration, cannot hide information in the Meeting Options panel or in the TelePresence or WebEx Advanced Settings dialog boxes, and cannot limit the number of video call-in participants the user can enter.

Although screen sharing (formerly called "desktop sharing" and application sharing are supported in CMR Hybrid meetings, some standard sharing features, such as file sharing, annotation, and whiteboard sharing, are not supported in CMR Hybrid meetings.

Starting with WBS29, recording is supported for CMR Hybrid meetings; however, it has the following known issues and limitations:

- CMR Hybrid meeting recordings will be in MP4 format. Video will be recorded at 360p.
- When users play back the recording, they can see screen sharing, video camera feeds, the participant, list, chat, and polling. However, if users download the recordings, the screen sharing and audio portion is in one MP4 file, and does not contain active speaker video camera feeds, the participant list, chat, and polling.

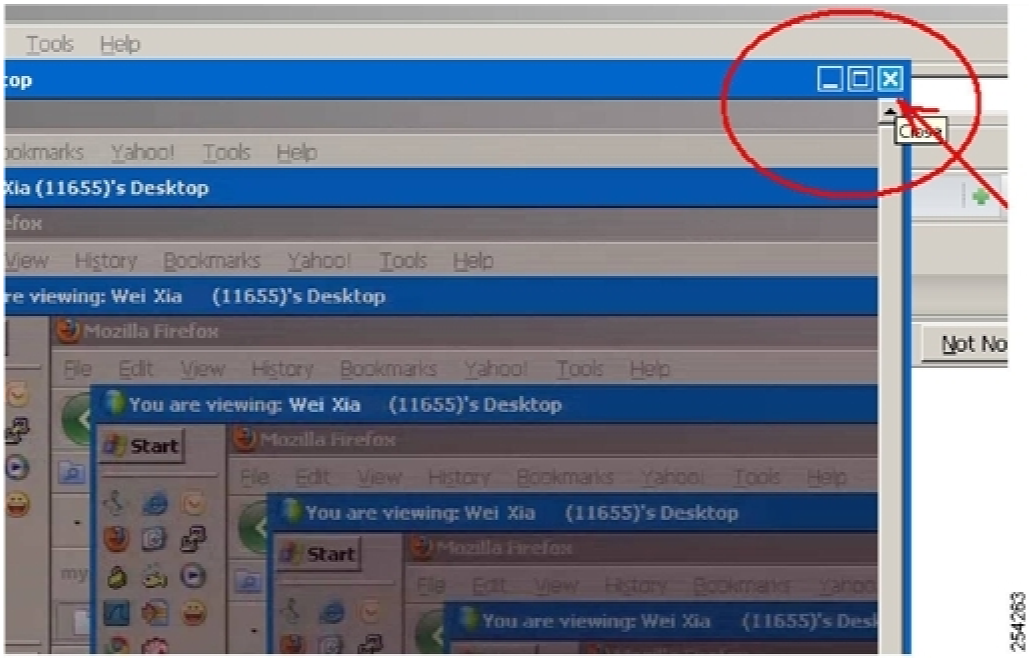
Managing System Behavior

Managing the Cisco WebEx Video View Window

A window cascading effect can occur if you plug in the presentation (VGA) cable between your PC and your while you have your Cisco WebEx video view panel open. To prevent this issue, close the Cisco WebEx video view application before connecting your presentation cable to your laptop to present.

If you receive a cascading screen, simply close the video view window, as shown in Figure 34: Cascading Cisco WebEx Video View Window [p.185].

Figure 34: Cascading Cisco WebEx Video View Window


Tools Help
Close
You are viewing: Wei Xia (11655)'s Desktop
Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
Start
Not No
254263

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.