



Cisco WebEx Enabled TelePresence Configuration Guide

April 30, 2013

Cisco TelePresence Management Suite (TMS) 14.3.1
Cisco WebEx Meeting Center WBS29

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

Text Part Number: OL-21352-02

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.

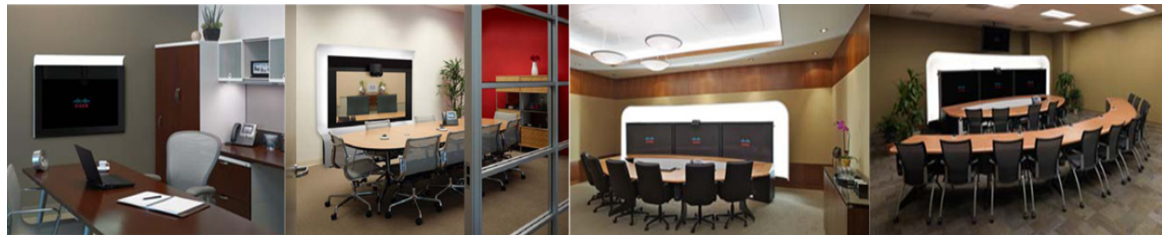
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

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.

Cisco WebEx Enabled TelePresence Configuration Guide
© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface	1
General Description	1
Audience and Scope	1
Cisco WebEx Features and Important Notes	2
Supported Features	2
Feature Limitations	3
Prerequisites	4
Document Organization	5
Related Documents	6
Obtaining Documentation and Submitting a Service Request	7
Information About the Cisco WebEx Enabled TelePresence Feature	1-1
Contents	1-1
Cisco WebEx Enabled TelePresence Experience	1-1
Scheduling the Meeting	1-1
Starting/Joining the Meeting	1-2
Cisco TelePresence Meeting Experience	1-2
Cisco WebEx Meeting Experience	1-2
Understanding How Cisco WebEx Enabled TelePresence is Deployed	1-6
SIP Video, Presentation and Audio	1-6
SIP Video, Presentation and PSTN Audio	1-7
Cisco TMS Scheduling Role	1-9
TelePresence Server and MCU Roles	1-9
Presentation Display Details for Multiple Presenters	1-9
Meeting Participant List	1-9
Ports and Protocols Used in WebEx Enabled TelePresence	1-10
Understanding Cisco WebEx Enabled TelePresence Scheduling Flow	1-10
Scheduling with the Cisco WebEx and TelePresence Integration to Outlook	1-11
Scheduling with the Cisco Smart Scheduler	1-13
Scheduling with the Cisco WebEx Scheduling Mailbox	1-15
Understanding Cisco WebEx Enabled TelePresence Call Flow	1-16
SIP Audio Call Flow	1-17
TSP Audio Call Flow with API Command to Unlock Waiting Room	1-19
TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host	1-21

WebEx Audio (PSTN) Call Flow 1-23

First-Time Configuration Checklist 2-1

- Contents 2-1
- Server and Site Access Checklist 2-1
- Configuration Task Checklist 2-3
 - Cisco MCU 2-3
 - Cisco TelePresence Server 2-4
 - Cisco Video Communications Server 2-4
 - Cisco Unified Communications Manager 2-4
 - Cisco TelePresence Management Suite 2-6
 - Cisco TelePresence Management Suite Extension for Microsoft Exchange 2-7
 - Cisco TelePresence Management Suite Provisioning Extension 2-8
 - Configure Audio for Cisco WebEx Enabled TelePresence 2-9
 - Cisco WebEx Site Administration 2-9

Configuring Cisco MCU and TelePresence Server 3-1

- Contents 3-1
- Introduction 3-1
- Required Settings for MCU 3-2
 - SIP 3-2
 - Content Mode 3-2
 - Video and Audio Codecs 3-2
 - Automatic Content Handover 3-3
- Recommended Settings for MCU 3-3
 - Automatically Make Content Channel Important 3-3
 - Outgoing Transcoded Codec 3-4
 - Adaptive Gain Control 3-4
 - Join and Leave Audio Notifications 3-5
 - Encryption 3-5
- Required Settings for TelePresence Server 3-5
 - SIP 3-6
 - Locally Managed Mode 3-6
 - Automatic Content Handover 3-6
- Recommended Settings for TelePresence Server 3-7
 - Display Setting 3-7

Configuring Call Control 4-1

- Introduction 4-1
- Configuring Cisco TelePresence Video Communication Server Control and Expressway 4-1

Prerequisites	4-2
Creating a New DNS Zone on VCS Expressway for WebEx	4-3
Configuring Traversal Zones for MCUs with Encryption Enabled	4-4
Configuring Cisco Unified Communications Manager	4-5
Prerequisites	4-5
Configuring a SIP Trunk Between Unified CM and VCS Control	4-5
Configuring Certificates on Cisco VCS Expressway	5-1
Introduction	5-1
VCS Expressway X8.1 Encryption Issue and Workarounds	5-1
Videos Available	5-2
Supported Certificates	5-2
Generating a Certificate Signing Request (CSR)	5-2
Installing the SSL Server Certificate on the VCS Expressway	5-6
Configuring the Trusted CA Certificate List on the VCS Expressway	5-11
Configuring the Trusted CA Certificate List on VCS Expressway X7.2.2	5-12
Configuring the Trusted CA Certificate List on VCS Expressway Upgraded from X7.2.2 to X8.1	5-18
Configuring the Trusted CA Certificate List on VCS Expressway X8.1	5-22
Configuring Cisco TelePresence Management Suite	6-1
Contents	6-1
Prerequisites	6-1
Configuring the Cisco WebEx Feature in Cisco TMS	6-2
Configuring WebEx Users in Cisco TMS	6-4
User Requirements for Scheduling WebEx-enabled Meetings	6-4
Configuring Automatic User Lookup from Active Directory	6-5
How WebEx Bookings Work	6-6
Configuring a Cisco WebEx Enabled TelePresence User in Cisco TMS	6-6
Configuring Port Reservations for MCU and TelePresence Server in Cisco TMS	6-7
Enabling Port Reservations for MCU	6-7
Enabling Port Reservations for TelePresence Server	6-7
Configuring Hybrid Content Mode for MCU in Cisco TMS	6-8
Configuring Lobby Screen for TelePresence Server in Cisco TMS	6-8
How the Lobby Screen Affects the First TelePresence Participant in a Meeting if the WebEx Welcome Screen is Disabled	6-8
Configuring Conference Settings in Cisco TMS	6-9
Default Setup and Teardown Buffers	6-9
Default Picture Mode	6-10
Conference Connection/Ending Options	6-10

- Configuring Single Sign On in Cisco TMS 6-11
 - Prerequisites 6-12
 - Configuring SSO in Cisco TMS 6-12
 - Generating a Certificate for WebEx 6-13
 - Enabling Partner Delegated Authentication on the WebEx site 6-16
 - Enabling SSO in Cisco TMS 6-17
 - Supported Configurations for TMS to Schedule on Behalf of the WebEx Host 6-18

Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange 7-1

- Contents 7-1
- Prerequisites 7-1
- Deployment Best Practices 7-2
- Scheduling Options with TMSXE 7-2
- Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook 7-2
 - Installing the Cisco TMS Booking Service 7-2
 - Setting Up Communication Between Your WebEx Site and TMSXE 7-5
- Configuring Cisco TMSXE for the WebEx Scheduling Mailbox 7-6
 - Configuring the WebEx Scheduling Mailbox in Microsoft Exchange 7-6
 - Adding the WebEx Mailbox to Cisco TMSXE 7-7
 - Additional Recommendations 7-7

Configuring Cisco TelePresence Management Suite Provisioning Extension 8-1

- Contents 8-1
- Prerequisites 8-1
- Introduction 8-2
- User Access to Cisco TMSPE 8-2
 - Creating a Redirect to Smart Scheduler 8-3
 - Access Rights and Permissions 8-3
 - Time Zone Display 8-3
- How Smart Scheduler Works 8-3
- Limitations 8-4

Configuring Audio 9-1

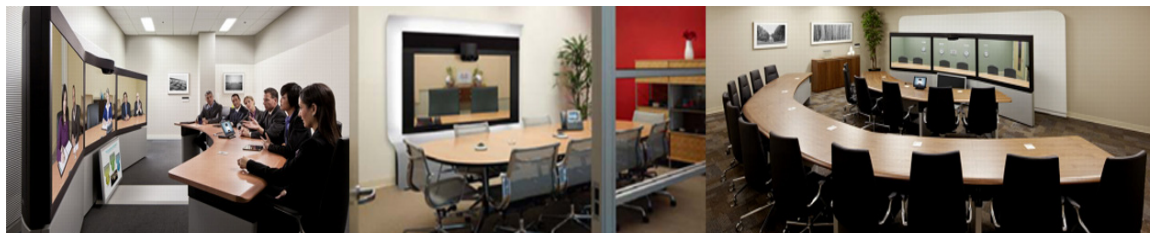
- Contents 9-1
- Prerequisites 9-1
- Configuring SIP Audio for Cisco WebEx Enabled TelePresence 9-2
 - Configuring the WebEx Site in Cisco TMS to Use SIP Audio 9-2
 - Enabling Hybrid Audio on the WebEx Site 9-3
- Configuring PSTN Audio for Cisco WebEx Enabled TelePresence 9-3

Configuring the WebEx Site in Cisco TMS to Use PSTN Audio	9-4
Enabling Hybrid Mode on the WebEx Site	9-4
Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx	9-4
Configuring TSP Audio for Cisco WebEx Enabled TelePresence	9-7
Configuring MACC Domain Index and Open TSP Meeting Room Webex Settings	9-8
Configuring the TSP Dial String	9-8
Configuring How the Conference is Opened	9-9
Configuring TSP Audio for the Meeting Organizer	9-11
Overview of TSP Audio Configuration and Meetings	9-12
Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account	10-1
Contents	10-1
Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account	10-1
Assigning the Meeting Center TelePresence Session Type	10-3
Network-Based Recording of WebEx Enabled TelePresence Meetings	10-6
Installing the WebEx and TelePresence Integration to Outlook	10-6
Setting the Time Zone and Language Preferences for a User's WebEx Account	10-8
Configuring TSP Audio for a User's WebEx Account	10-9
Where to Go Next	10-9
Scheduling Cisco WebEx Enabled TelePresence Meetings	11-1
Contents	11-1
Introduction	11-2
Scheduling WebEx Enabled TelePresence Meetings in Cisco TMS	11-3
Information, Tips and Known Issues About WebEx Enabled TelePresence Meetings	11-5
Cisco TMS	11-5
MCU and TelePresence Server	11-6
Endpoints	11-6
TMSXE	11-7
WebEx	11-7
Troubleshooting	12-1
Contents	12-1
Verifying and Testing	12-1
Cisco WebEx Site Administration Online Help	12-1
Troubleshooting Tips	12-1
Problems with Scheduling a Meeting	12-2
Problems with Starting or Joining a Meeting	12-3
Problems During a Meeting	12-4
Problems with a TSP Audio Meeting	12-7

Problems with TelePresence Server and MCU 12-9

Managing System Behavior 12-10

Managing the Cisco WebEx Video View Window 12-10



Preface

Revised: April 2014

This preface describes the purpose, audience, organization, and conventions of the Cisco WebEx Enabled TelePresence Configuration Guide - TMS 14.3.1 - WebEx Meeting Center WBS29 and provides information about new features and how to obtain related documentation.

This preface describes the following topics:

- [General Description, page 1](#)
- [Audience and Scope, page 1](#)
- [Cisco WebEx Features and Important Notes, page 2](#)
- [Prerequisites, page 4](#)
- [Document Organization, page 5](#)
- [Related Documents, page 6](#)
- [Obtaining Documentation and Submitting a Service Request, page 7](#)

General Description

This document describes how to configure Cisco TelePresence applications for Cisco WebEx-to-Cisco Telepresence interoperability. The Cisco WebEx Enabled TelePresence Configuration Guide - TMS 14.3.1 - WebEx Meeting Center WBS29 describes how to manage and monitor scheduled meeting interoperability between Cisco TelePresence System (CTS), Cisco TelePresence Server or MCU multipoint meetings, Cisco TMS, Cisco Unified Communications Manager (Cisco Unified CM), Cisco Video Communication Server (VCS) and the Cisco WebEx Meeting Center.

Audience and Scope

The *Cisco WebEx Enabled TelePresence Configuration Guide - TMS 14.3.1 - WebEx Meeting Center WBS29* is directed to administrators who will be configuring the TelePresence Server, MCU, Cisco TMS, Cisco VCS and/or the Cisco Unified CM to use Cisco WebEx features in Cisco TelePresence meetings.

Cisco WebEx Features and Important Notes

This section contains the following feature information:

- [Supported Features, page 2](#)
- [Feature Limitations, page 3](#)

Supported Features

Cisco WebEx Enabled TelePresence provides the following key features:

- Two-way video sharing with up to 720p screen resolution between the WebEx client and TelePresence endpoints
- Integrated audio and presentation sharing — including application and desktop content sharing capability for all users in a meeting
- Integrated meeting scheduling using TelePresence Management Suite (Cisco TMS), which allows you to easily schedule Cisco WebEx Enabled TelePresence meetings
- Secure call control and connectivity enabled by media encryption provided by Cisco VCS Expressway
- Interoperability with third-party telepresence endpoints

Table 1 lists Cisco WebEx Enabled TelePresence features.

Table 1 *Cisco WebEx Enabled TelePresence Features*

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

Table 1 Cisco WebEx Enabled TelePresence Features

Supported Feature	Description
Scheduling	<p>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.</p> <p>You can start the WebEx portion of a Cisco WebEx Enabled TelePresence 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.</p> <p>Note Only scheduled meetings are supported for Cisco WebEx Enabled TelePresence Interoperability; non-scheduled TelePresence participants who want to join a Cisco WebEx enabled TelePresence meeting, must manually dial into the conference (MCU/TelePresence Server) bridge. The meeting organizer can reserve ports for video dial-in participants when scheduling the meeting.</p> <p>See the Cisco TelePresence Management Suite Administrator Guide for meeting scheduling information.</p>
Sharing	<p>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.</p> <p>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.</p> <p>The resolution that endpoints are capable of sending may vary depending on the endpoint model, but the TelePresence Server/MCU will transcode the presentation and send it to the WebEx cloud at 1024x768 resolution.</p> <p>Note The Cisco TelePresence user that is sharing with the video display cable must exit the Cisco WebEx Meeting Center client on their laptop before connecting the video display cable. If they do not, a window cascading effect can occur. For more information, refer to Chapter 12, “Managing the Cisco WebEx Video View Window”.</p>
Two-way Video	<p>Video quality is sent best effort from the Cisco TelePresence endpoint to Cisco WebEx and from Cisco WebEx to the Cisco TelePresence endpoint.</p> <p>The video from the CTS participants in the meeting are forwarded to the Cisco WebEx network, where they will be seen by Cisco WebEx participants along with other Cisco WebEx participants. 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.</p> <p>Presentations from the Cisco WebEx client are displayed on the local CTS projector, presentation display or with Presentation-in-Picture (PiP), depending on the capabilities of your CTS.</p> <p>Note All Cisco WebEx-enabled TelePresence meetings require the use of a Cisco TelePresence Server or MCU.</p>

Feature Limitations

For a complete list of limitations and known issues for Cisco WebEx Enabled TelePresence, refer to the Cisco WebEx Enabled TelePresence release notes.

Prerequisites

Table 2 lists Cisco WebEx Enabled TelePresence feature prerequisites.

Table 2 Cisco WebEx with the Cisco TelePresence System Prerequisites


Requirement	Description
Cisco TelePresence Management Suite (Cisco TMS)	Cisco TMS is required for scheduling Cisco WebEx Enabled TelePresence meetings. Release 14.3.1 or later is required. (Release 14.3 or later is also required for support of TSP audio with Cisco TelePresence Server.)
Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE)	Cisco TMSXE is required for scheduling Cisco WebEx Enabled TelePresence meetings through Microsoft Outlook using either the WebEx Productivity Tools Plug-in or WebEx Scheduling Mailbox Scheduling. Release 3.1 or later is required.
Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE)	Cisco TMSPE is required for scheduling Cisco WebEx Enabled TelePresence meetings using Smart Scheduler. Release 1.1 or later is required. Note Use of Smart Scheduler does not require the TMS provisioning option key.
Cisco TelePresence Video Communication Server (VCS)	VCS Control and Expressway are a required as the call control solution. Release X7.2.2 or later is required.  Caution Customers using Static NAT on VCS Expressway X7.2.2 are highly recommended to not upgrade to X8.1. Because VCS Expressway X8.1 uses the Ethernet 2 IP address for the media part in SDP, the media part of calls will fail. If you are already using static NAT with X8.1, refer to the recommended workarounds in Chapter 5, “VCS Expressway X8.1 Encryption Issue and Workarounds” .
Cisco Unified Communications Manager (Unified CM)	Unified CM is an optional call control solution that can be used with VCS for deployments with endpoints registered to Unified CM. Release 8.6.2 or higher is required. 9.1.1 is recommended.
Cisco TelePresence Server	TelePresence Server can be used as a conference bridge for Cisco WebEx Enabled TelePresence meetings. Release 3.0 or later is required. Release 3.1 or later with a Third-Party Interop key is required for support of TSP audio.
Cisco TelePresence MCU	Cisco TelePresence MCU can be used as a conference bridge for Cisco WebEx Enabled TelePresence meetings. Release 4.4 or later is required.
Provisioning—Cisco TelePresence with Cisco WebEx.	<ol style="list-style-type: none"> 1. The Cisco WebEx Meeting Center site must be running release T28.10 or higher with the latest service pack. 2. The Cisco WebEx site must be configured to support Cisco TelePresence Integration. See Chapter 10, “Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account” for more information.

Table 2 Cisco WebEx with the Cisco TelePresence System Prerequisites

Requirement	Description
Supported Endpoints	Any endpoint supported by TelePresence Server or MCU can join a Cisco WebEx Enabled TelePresence meeting.
Account Validation—Meeting scheduler's Cisco WebEx account.	<p>Each user who is scheduling Cisco WebEx Enabled TelePresence meetings in Cisco TMS, must have a host account on the WebEx site.</p> <ol style="list-style-type: none"> 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. <p>Note WebEx password is not required if Single-Sign-On (SSO) is configured in TMS. See Chapter 6, “Configuring Cisco TelePresence Management Suite” for more information.</p>
Bandwidth and CPU power—Recommendation for good video quality and integrating the Cisco TelePresence network with Cisco WebEx.	<p>Network bandwidth should be at least 1.1 Mbps upstream between the MCU/TelePresence Server and WebEx. For example, if you are anticipating 5 simultaneous Cisco WebEx calls, you will need to have five 1.1 Mbps bandwidth instances.</p> <p>Suggested CPU power (depends on running applications) is dual core CPU, 2.5 GHz memory running at least 2G.</p>
Cisco WebEx Client Resource Requirements—Expected resource allocation per meeting.	For detailed requirements, refer to the Cisco WebEx Enabled TelePresence release notes .

Document Organization

Information about configuring and using the Cisco WebEx Enabled TelePresence is provided in the following chapters:

- [Chapter 1, “Information About the Cisco WebEx Enabled TelePresence Feature”](#)
- [Chapter 2, “First-Time Configuration Checklist”](#)
- [Chapter 3, “Configuring Cisco MCU and TelePresence Server”](#)
- [Chapter 4, “Configuring Call Control”](#)
- [Chapter 5, “Configuring Certificates on Cisco VCS Expressway”](#)
- [Chapter 6, “Configuring Cisco TelePresence Management Suite”](#)
- [Chapter 7, “Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange”](#)
- [Chapter 8, “Configuring Cisco TelePresence Management Suite Provisioning Extension”](#)
- [Chapter 9, “Configuring Audio”](#)
- [Chapter 10, “Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account”](#)
- [Chapter 11, “Scheduling Cisco WebEx Enabled TelePresence Meetings”](#)
- [Chapter 12, “Troubleshooting”](#)

Related Documents

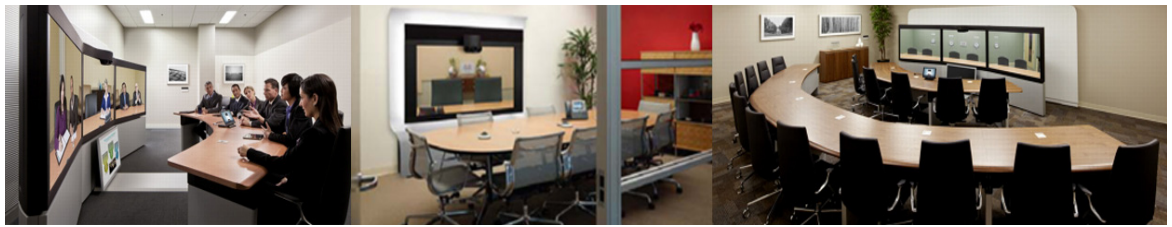
Related Topic	Document Link
Cisco TelePresence Documentation	
Cisco TelePresence Management Suite	<ul style="list-style-type: none"> • Cisco TelePresence Management Suite
Cisco TelePresence Video Communication Server (VCS)	<ul style="list-style-type: none"> • Cisco TelePresence Video Communication Server
Cisco Unified Communications Manager (Unified CM)	<ul style="list-style-type: none"> • Cisco Unified Communications Manager
Cisco TelePresence Server	<ul style="list-style-type: none"> • Cisco TelePresence Server
Cisco TelePresence MCU	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Refer to Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account.
Cisco WebEx Enabled TelePresence Documentation	
Information for meeting organizers on how to schedule WebEx Enabled TelePresence meetings	<ul style="list-style-type: none"> • 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.



CHAPTER 1

Information About the Cisco WebEx Enabled TelePresence Feature

Revised: August 2014

Contents

This chapter provides an overview of the Cisco WebEx Enabled TelePresence solution. It contains the following sections:

- [Cisco WebEx Enabled TelePresence Experience, page 1-1](#)
- [Understanding How Cisco WebEx Enabled TelePresence is Deployed, page 1-6](#)
- [Understanding Cisco WebEx Enabled TelePresence Scheduling Flow, page 1-10](#)
- [Understanding Cisco WebEx Enabled TelePresence Call Flow, page 1-16](#)

Cisco WebEx Enabled TelePresence Experience

This section contains the following information about the Cisco WebEx Enabled TelePresence meeting experience:

- [Scheduling the Meeting, page 1-1](#)
- [Starting/Joining the Meeting, page 1-2](#)
- [Cisco TelePresence Meeting Experience, page 1-2](#)
- [Cisco WebEx Meeting Experience, page 1-2](#)

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, refer to [Chapter 11, “Scheduling Cisco WebEx Enabled TelePresence Meetings”](#).

Starting/Joining the Meeting

The meeting is started 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 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 both WebEx participants and telepresence participants.

The Cisco WebEx bridging feature integrates the Cisco WebEx conferencing server with multipoint meetings on the Cisco TelePresence MCU 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 speaker in the Cisco TelePresence system is streamed to the Cisco WebEx Web client.

Cisco WebEx Meeting Experience

Remote participants join the Cisco WebEx meeting by logging in to the Cisco WebEx Meeting Center Web and/or mobile clients*. Content shared from the Cisco TelePresence endpoint is displayed automatically in the Cisco WebEx Meeting Center clients and Cisco WebEx participants can share their desktop or application with Cisco Telepresence endpoints. Cisco WebEx users see the live video of the actively speaking Cisco TelePresence participant or WebEx participant. WebEx participants can go into Full Screen view to see all the other WebEx and TelePresence participants in the meeting. When in full screen mode, WebEx participants can see all WebEx participants who have their video turned on. While in full-screen mode, participants will see video sent from TelePresence when a TelePresence participant is the active speaker. Cisco WebEx users also see an integrated list of all Cisco WebEx meeting participants. The WebEx annotation feature is supported. WebEx participants can annotate using the standard WebEx Meeting Center client 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 1-1 on page 1-4) and in the row of WebEx participants in Full Screen view (Figure 1-2 on page 1-5). This indicates that it is a Cisco WebEx Enabled TelePresence 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 Cisco WebEx participants to share their presentation with TelePresence participants, they must do the following:

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

* For a list supported mobile clients, refer to the Cisco WebEx Enabled TelePresence 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

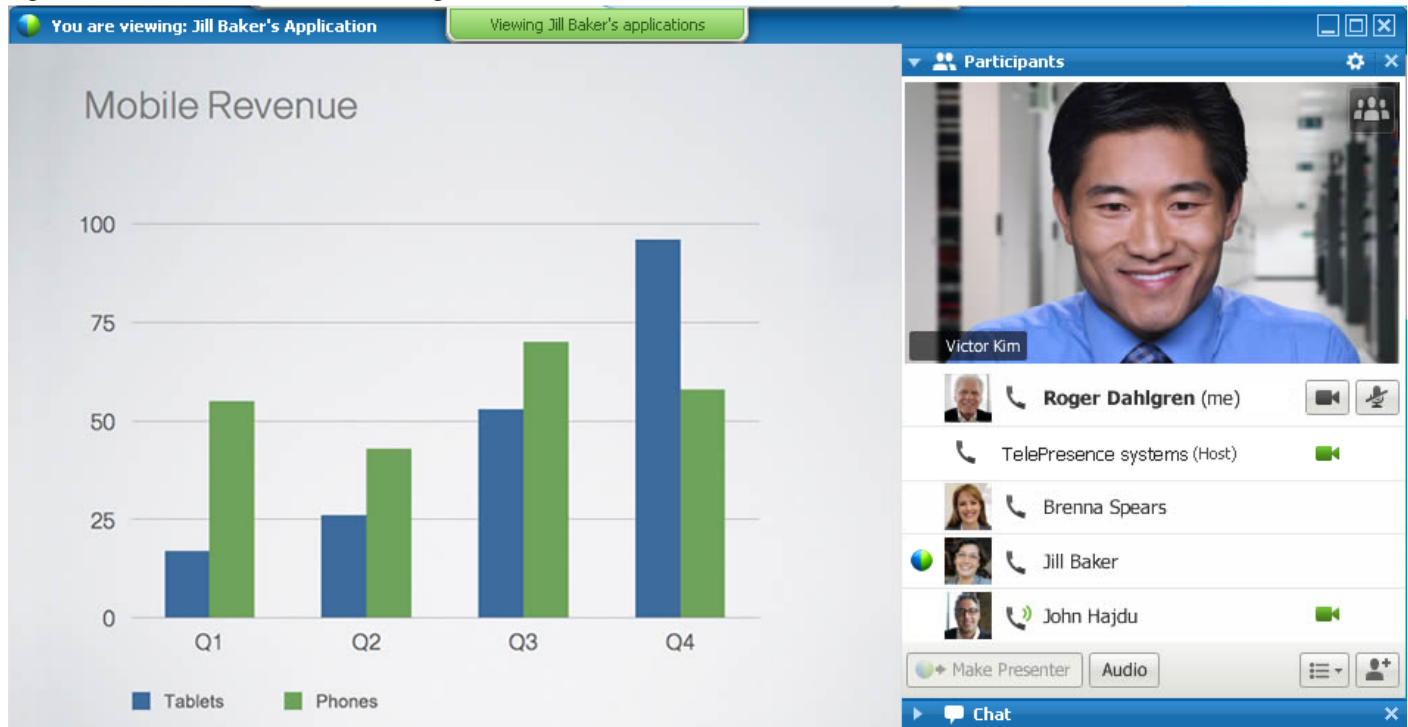
When attending the meeting using the WebEx Meeting Center web client (Windows or Mac), you have two basic ways to experience the meeting:

- [Default View, page 1-3](#)
- [Full Screen View, page 1-4](#)

Default View

When you log in to the meeting, the WebEx client displays the default view (see Figure 1-1). 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 1-1 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 1-2). When in Full Screen mode, the presentation is not visible.

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 Figure 1-3 for an example of Active Presence enabled by default on the TelePresence Server. MCU sends a full screen layout.

Figure 1-2 Cisco WebEx Meeting - Full Screen View



Figure 1-3 Cisco WebEx Meeting - Full Screen View with Cisco TelePresence Server in Active Presence Mode



Understanding How Cisco WebEx Enabled TelePresence is Deployed

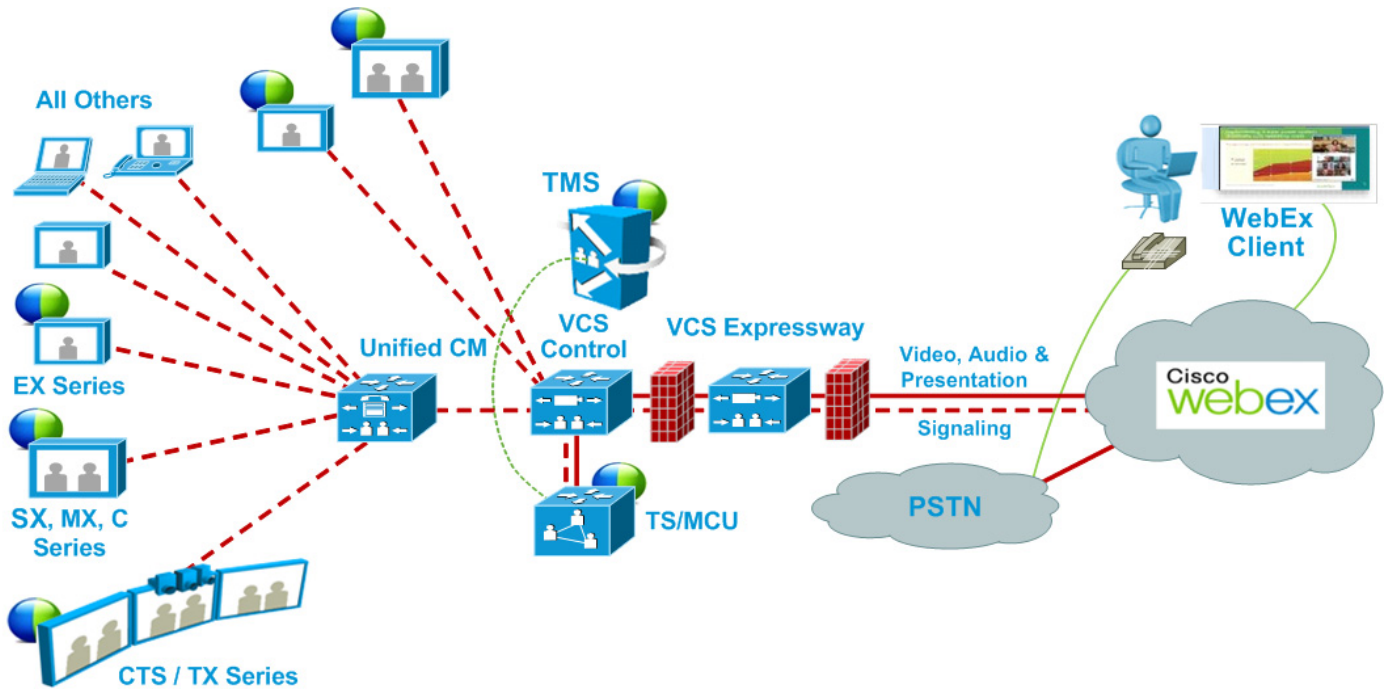
There are three possible network topologies for Cisco WebEx Enabled TelePresence:

- [SIP Video, Presentation and Audio, page 1-6](#)
- [SIP Video, Presentation and PSTN Audio, page 1-7:](#)
 - Using a gateway registered to Unified CM
 - Using a gateway registered to Cisco VCS Control

SIP Video, Presentation and Audio

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 1-4 Network Topology - SIP Video, Audio and Presentation



SIP Video, Presentation and PSTN Audio

WebEx is deployed using WebEx Audio using PSTN. Only main video and content is negotiated through the 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 1-5](#).
- Using a PSTN gateway registered to VCS - See [Figure 1-6](#).



Note

This deployment type is not supported with Cisco TelePresence Server.

Figure 1-5 Network Topology - SIP Video and Presentation with PSTN Audio Using Unified CM

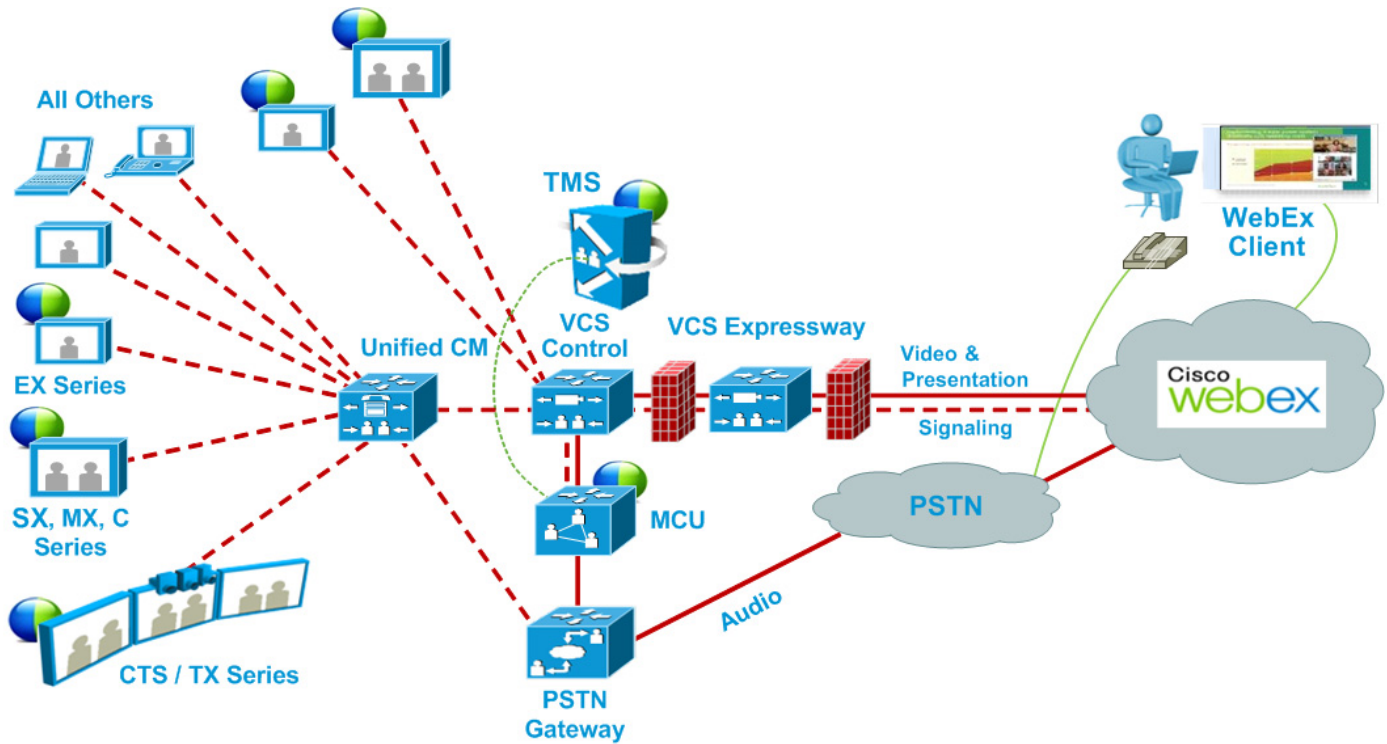
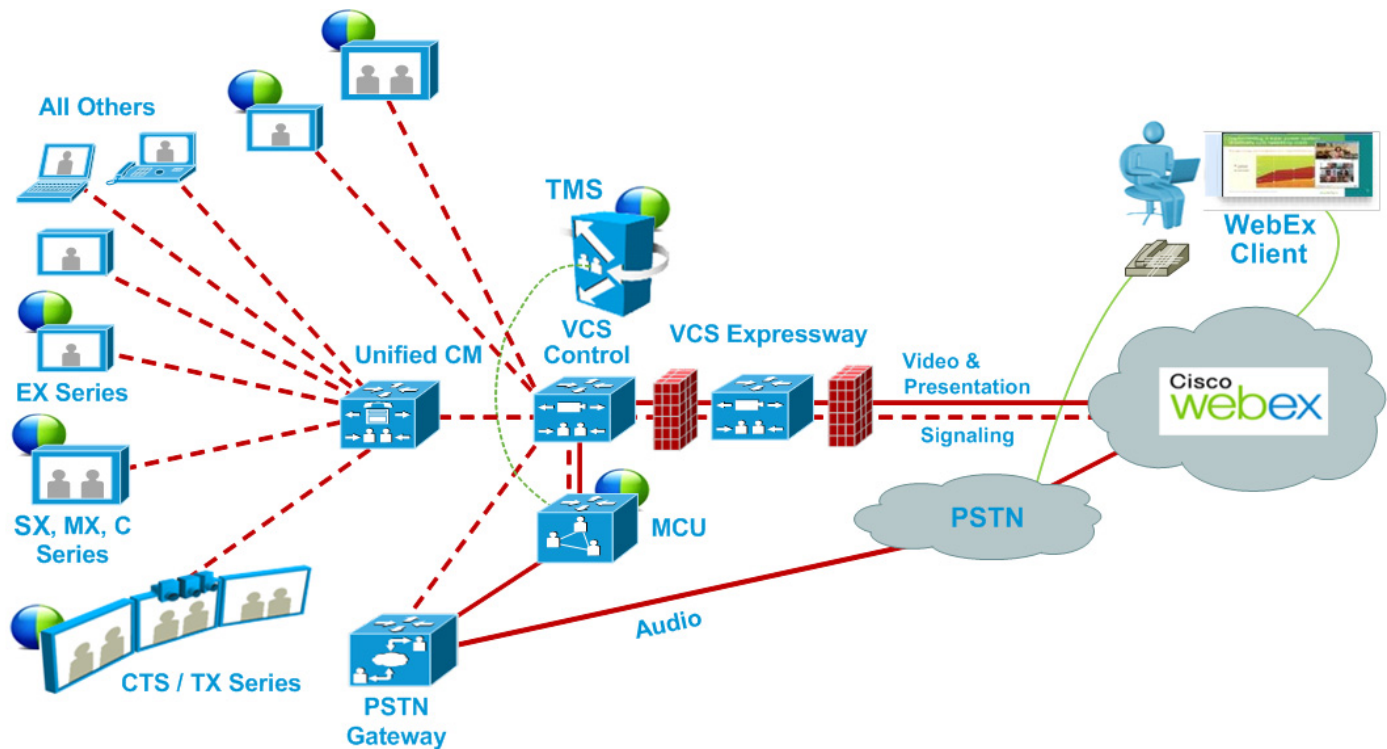


Figure 1-6 Network Topology - SIP Video and Presentation with PSTN Audio Using VCS Control



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/TelePresence Server sends a single transcoded video stream to the WebEx Meeting Center client.

The MCU/TelePresence Server will send a single mixed audio stream of the TelePresence meeting participants to the WebEx cloud. Likewise, the MCU/TelePresence Server 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 (1024x768) 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.

Presentation Display Details for Multiple Presenters

For TelePresence users 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 users 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 users 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 Participant List

The TelePresence participant list, a roster of endpoint names currently connected to the 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 WebEx Enabled TelePresence

The following ports and protocols are used between different components of the WebEx Enabled TelePresence solution.

Table 1-1 Ports and Protocols Used in WebEx Enabled TelePresence

Component Communication	Port and Protocol Used
TMS to WebEx cloud	Ephemeral port using TLS.443
WebEx and TelePresence Integration to Outlook to TMSXE	Ephemeral port using TLS.443
VCS Expressway to WebEx cloud	TLS and UDP ports 9000 and 9001 for media

Understanding Cisco WebEx Enabled TelePresence Scheduling Flow

This section describes what takes place when a Cisco WebEx Enabled TelePresence Meeting is scheduled using the following:

- [Scheduling with the Cisco WebEx and TelePresence Integration to Outlook, page 1-11](#)
- [Scheduling with the Cisco Smart Scheduler, page 1-13](#)
- [Scheduling with the Cisco WebEx Scheduling Mailbox, page 1-15](#)



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 1-7 Cisco WebEx and TelePresence Integration to Outlook Scheduling Flow

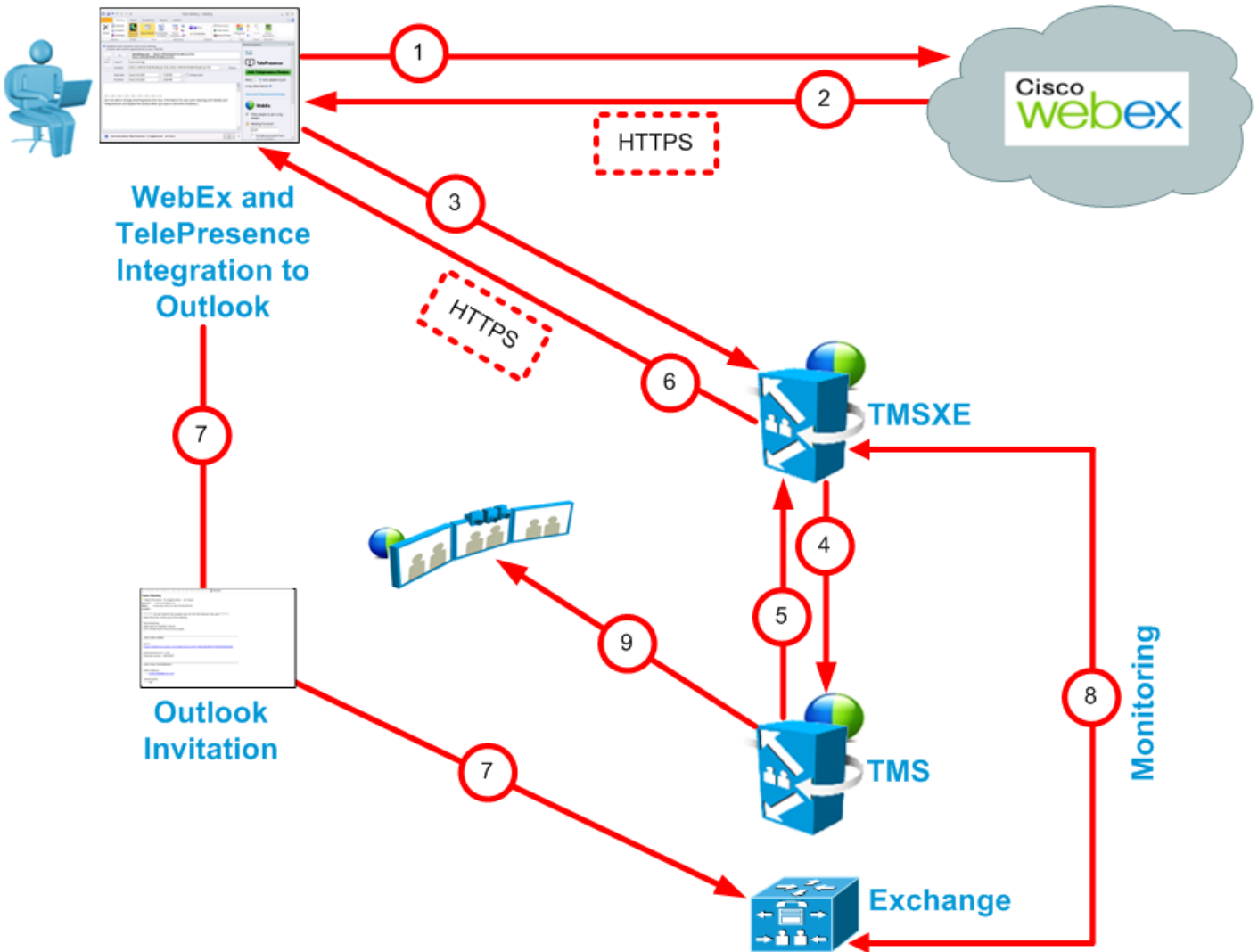


Table 1-2 Cisco WebEx and TelePresence Integration to Outlook Scheduling Steps

Step #	Description
1	User books meeting with Cisco WebEx and TelePresence Integration to Outlook. <ul style="list-style-type: none"> • Adds users • Adds rooms • Meeting request is sent to WebEx and books the WebEx portion of meeting.
2	WebEx responds with meeting information: <ul style="list-style-type: none"> • Date and time of meeting • Meeting subject • Audio dial-in information <ul style="list-style-type: none"> – 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 1-8 Cisco WebEx Smart Scheduler Scheduling Flow

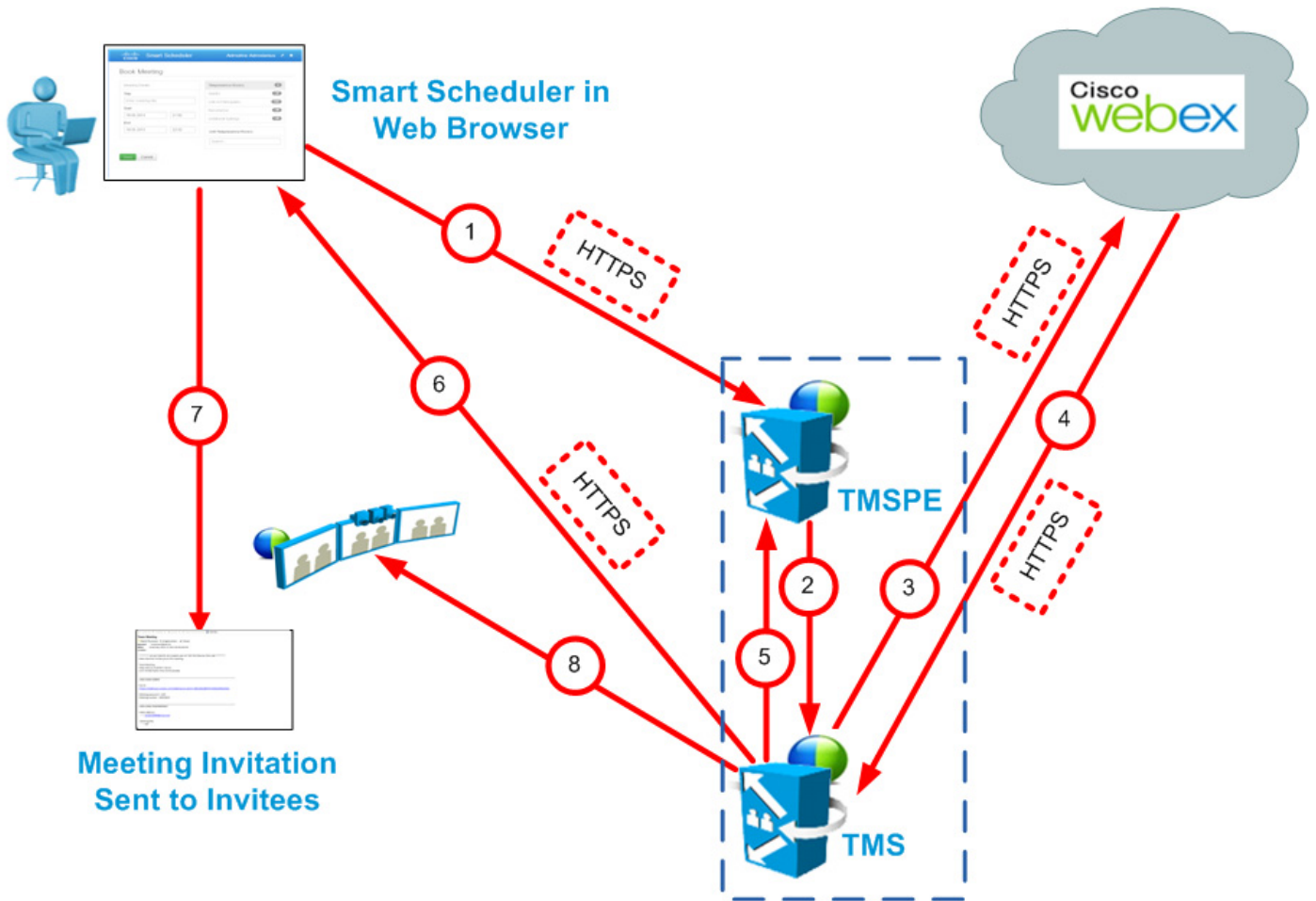


Table 1-3 Cisco Smart Scheduler Scheduling Steps

Step #	Description
1	User books meeting with Smart Scheduler. <ul style="list-style-type: none"> • Adds rooms • Adds WebEx • Clicks Save.
2	<ul style="list-style-type: none"> • TMSPE sends a booking request to TMS.
3	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Date/time of the meeting • Meeting subject • Audio dial-in information <ul style="list-style-type: none"> – 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 1-9 Cisco WebEx Scheduling Mailbox Scheduling Flow

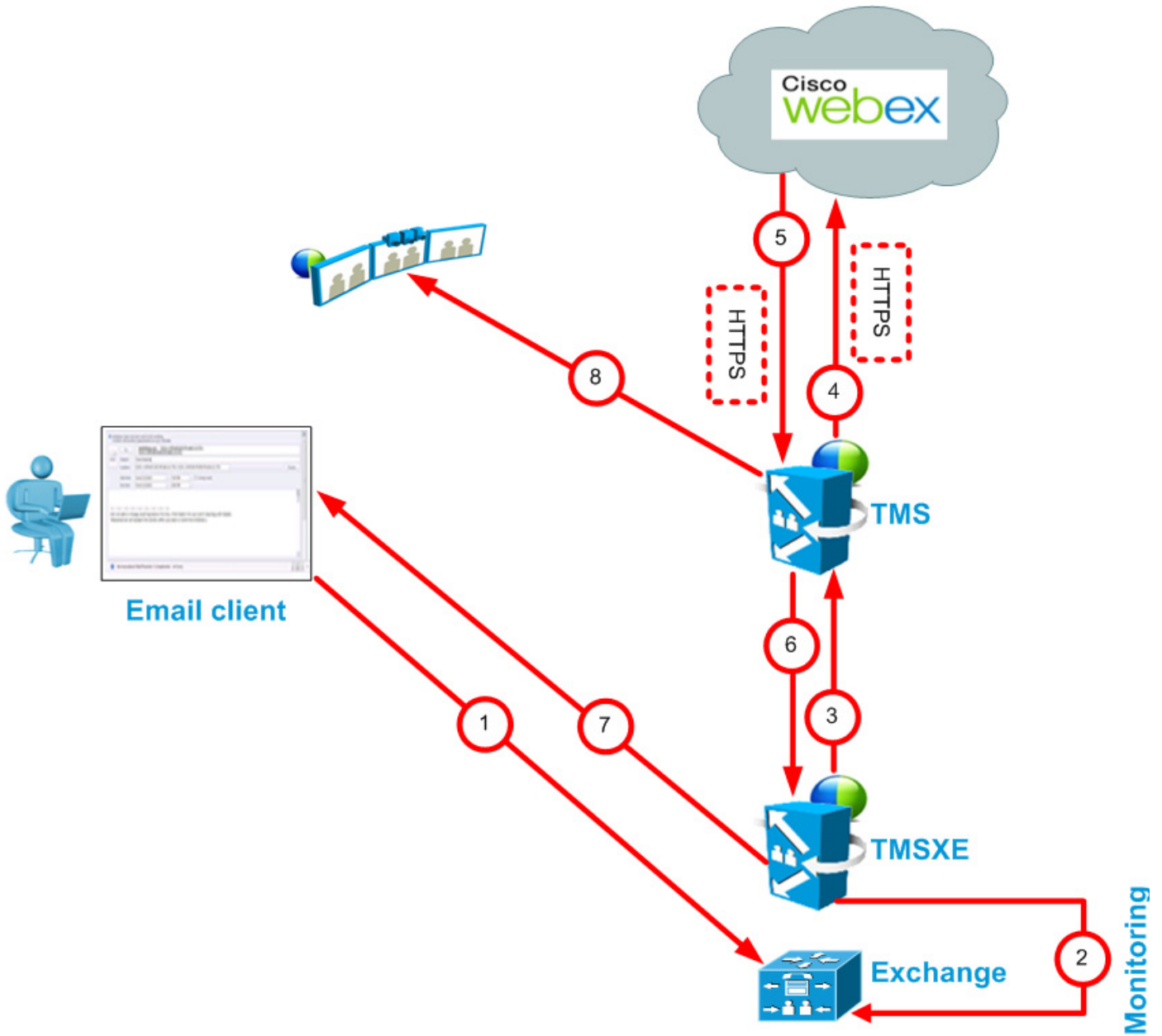


Table 1-4 Cisco WebEx Scheduling Mailbox Scheduling Steps

Step #	Description
1	User books meeting in email/calendar client supported by Microsoft Exchange: <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • Date/time of the meeting • Meeting subject • Audio dial-in information <ul style="list-style-type: none"> – 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 Cisco WebEx Enabled TelePresence Call Flow

This section describes the call flow of the following Cisco WebEx Enabled TelePresence Meetings:

- [SIP Audio Call Flow, page 1-17](#)
- [TSP Audio Call Flow with API Command to Unlock Waiting Room, page 1-19](#)
- [TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host, page 1-21](#)
- [WebEx Audio \(PSTN\) Call Flow, page 1-23](#)

SIP Audio Call Flow

Figure 1-10 SIP Audio Call Flow

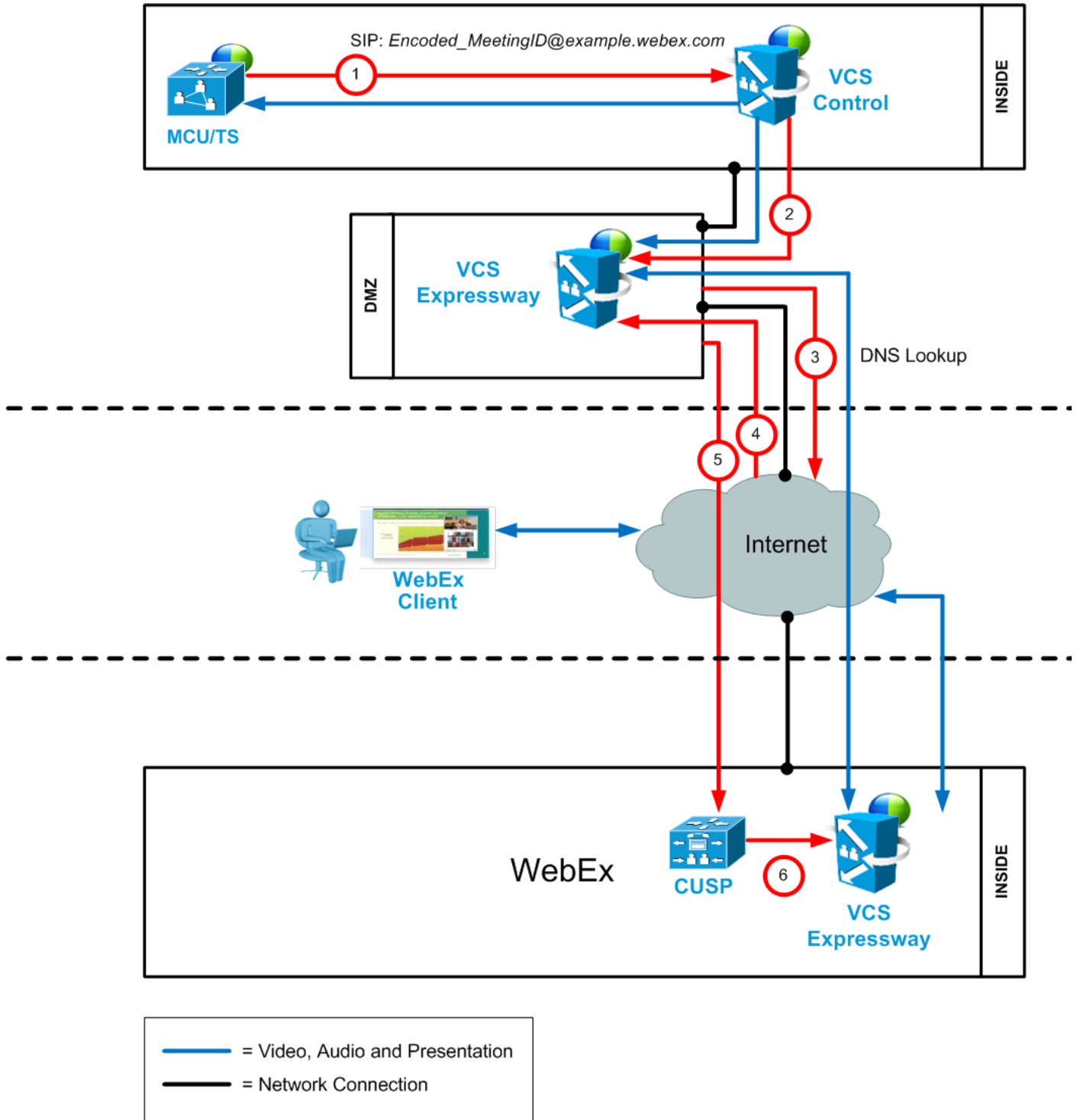


Table 1-5 SIP Audio Call Flow Steps

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

TSP Audio Call Flow with API Command to Unlock Waiting Room

Figure 1-11 TSP Audio Call Flow with API Command to Unlock Waiting Room

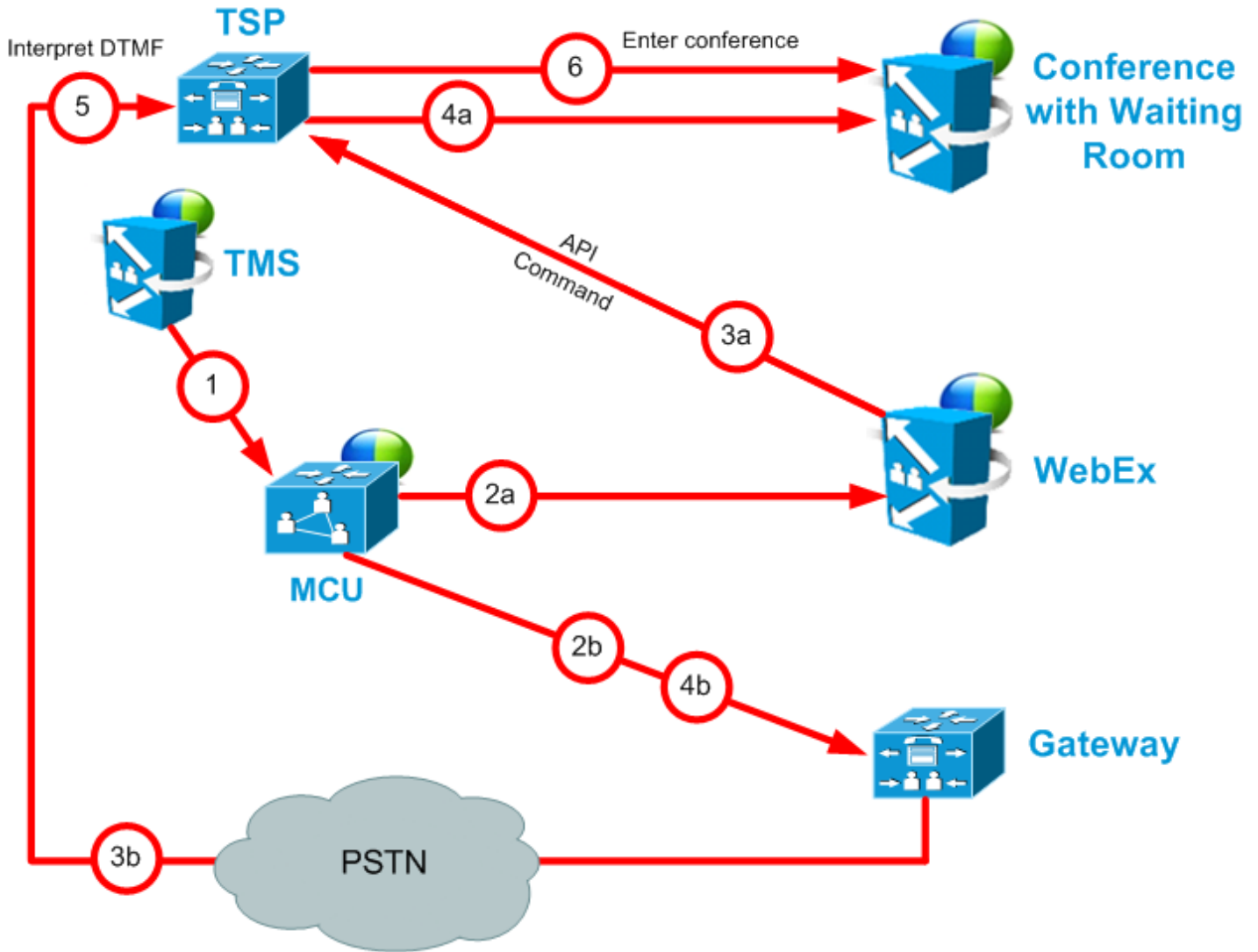


Table 1-6 TSP Audio Call Flow with API Command to Unlock Waiting Room Steps

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 Figure 1-10 for details).
2b	At the same time as step 2a, MCU/TelePresence Server dials PSTN call-in number for WebEx.

Step #	Description
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.
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 1-12 TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host

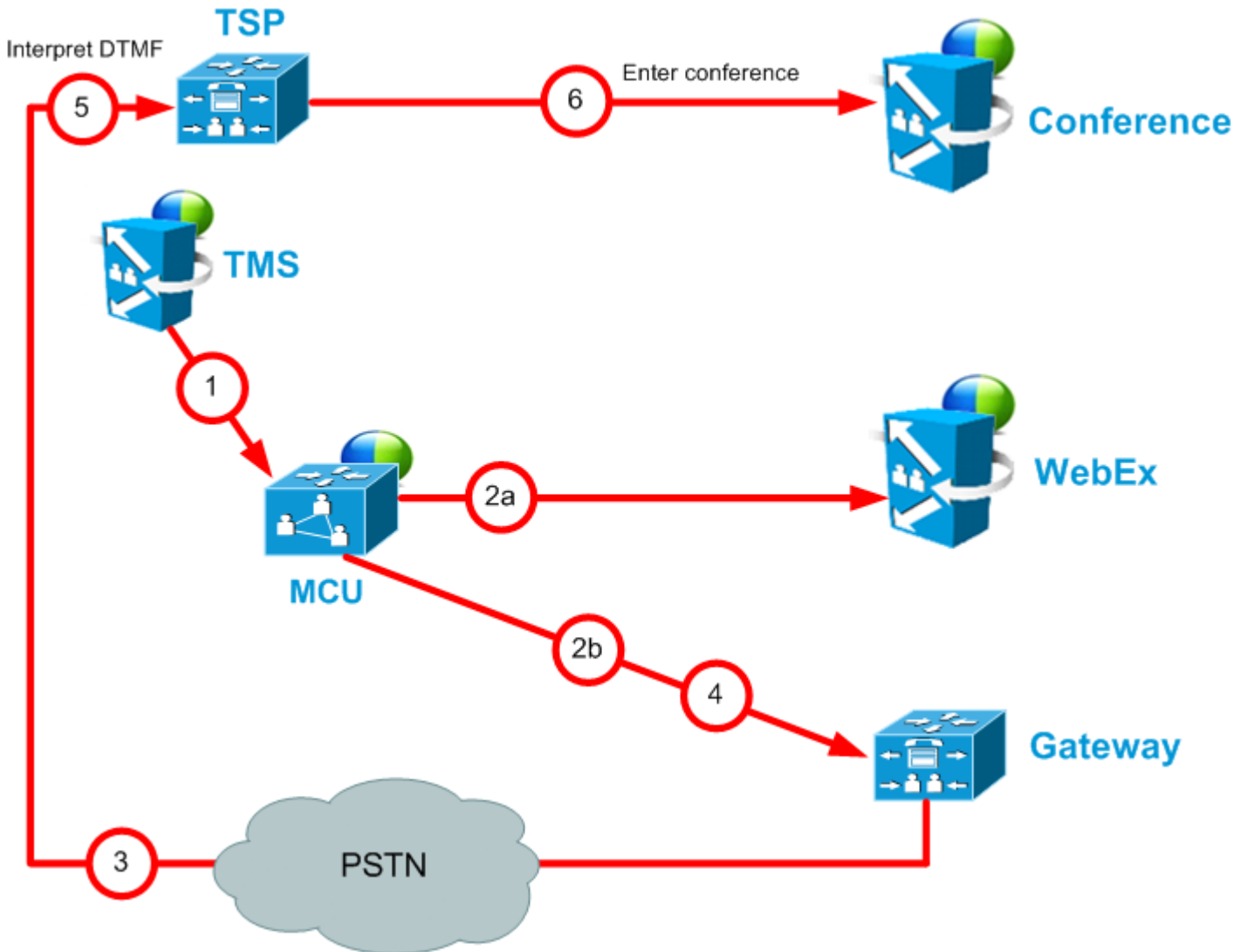


Table 1-7 TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host Steps

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 Figure 1-10 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.

Step #	Description
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 1-13 WebEx Audio (PSTN) Call Flow

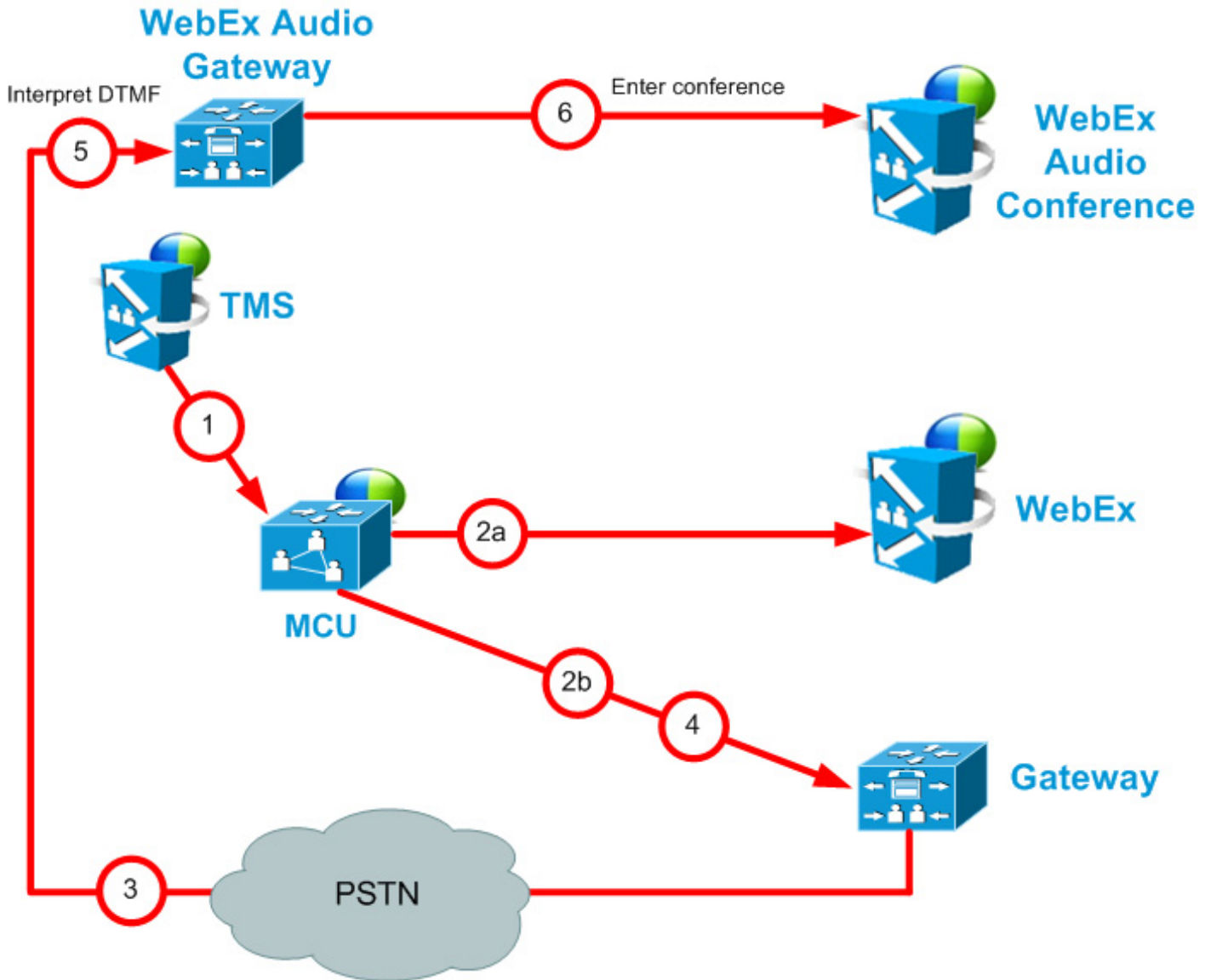
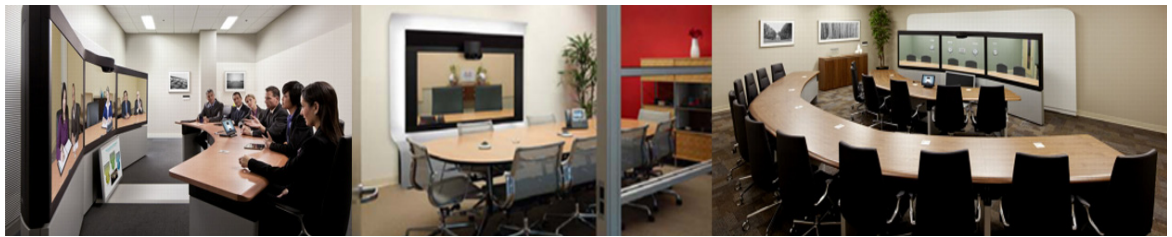


Table 1-8 WebEx Audio Call Flow Steps

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 Figure 1-10 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.

Step #	Description
5	WebEx receives the DTMF tones.
6	WebEx places the MCU into the audio conference.



CHAPTER 2

First-Time Configuration Checklist

Revised: December 2013

Contents

This chapter describes items and configuration tasks required to deploy Cisco WebEx Enabled TelePresence. It contains the following sections:

- [Server and Site Access Checklist, page 2-1](#)
- [Configuration Task Checklist, page 2-3](#)

Server and Site Access Checklist

[Table 2-1](#) describes information you must have before you can configure Cisco WebEx Enabled TelePresence for the first time.

Table 2-1 *Make Sure You Have the Following*

What You Need	Description and Source	✓
WebEx Site URL	URL for the Cisco WebEx site. Source —Provided by the Cisco WebEx Account Team. Example — <i>https://example.webex.com/example</i> Detailed Instructions — Configuring Cisco TelePresence Management Suite .	
WebEx Site Hostname	Hostname of WebEx site used by the customer. Source —Provided by the Cisco WebEx Account Team. Example —“example.webex.com” Detailed Instructions — Configuring Cisco TelePresence Management Suite	

Table 2-1 Make Sure You Have the Following

What You Need	Description and Source	✓
WebEx Site Administration URL	<p>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.</p> <p>Source—Provided by the Cisco WebEx Account Team.</p> <p>Example—“https://example.webex.com/admin”</p> <p>Detailed Instructions— Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account</p>	
Cisco WebEx Administrator username	<p>Cisco WebEx Site Administrator account username.</p> <p>Source—Provided by the Cisco WebEx Account Team.</p> <p>Example—“webexAdmin”</p> <p>Detailed Instructions— Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account</p>	
(Optional) Certificate pair, including public certificate and private key from TMS.	<p>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.</p> <p>Detailed Instructions— Configuring Single Sign On in Cisco TMS</p>	
Client/server certificate for VCS Expressway.	<p>Because the call leg between the 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.</p> <p>Detailed Instructions— Creating a New DNS Zone on VCS Expressway for WebEx and Configuring Certificates on Cisco VCS Expressway.</p>	

Configuration Task Checklist

You can choose the order in which you wish to configure Cisco TelePresence components for Cisco WebEx Enabled TelePresence; 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:
 - [Cisco MCU, page 2-3](#)
 - [Cisco TelePresence Server, page 2-4](#)
2. Call control:
 - [Cisco Video Communications Server, page 2-4](#)
 - [Cisco Unified Communications Manager, page 2-4](#)
3. Scheduling:
 - [Cisco TelePresence Management Suite, page 2-6](#)
 - [Cisco TelePresence Management Suite Extension for Microsoft Exchange, page 2-7](#)
 - [Cisco TelePresence Management Suite Provisioning Extension, page 2-8](#)
4. Audio:
 - [Configure Audio for Cisco WebEx Enabled TelePresence, page 2-9](#)
5. WebEx site:
 - [Cisco WebEx Site Administration, page 2-9](#)

Cisco MCU

Table 2-2 Checklist — Configuring Cisco WebEx Enabled TelePresence on the MCU for the First Time

Go to: Chapter 3, "Configuring Cisco MCU and TelePresence Server"			
	Task	Detailed Instructions	✓
Step 1	Configure SIP	SIP, page 3-2	
Step 2	Configure the Content Mode .	Content Mode, page 3-2	
Step 3	Configure the Video and Audio Codecs .	Video and Audio Codecs, page 3-2	
Step 4	Configure the Automatic Content Handover .	Automatic Content Handover, page 3-3	
Step 5	Configure Optional Recommended Settings : <ul style="list-style-type: none"> • Automatically Make Content Channel Important • Outgoing Transcoded Codec • Adaptive Gain Control • Join and Leave Audio Notifications • Encryption 	Recommended Settings for MCU, page 3-3	

Cisco TelePresence Server

Table 2-3 Checklist — Configuring Cisco WebEx Enabled TelePresence on the TelePresence Server for the First Time

Go to: Chapter 3, “Configuring Cisco MCU and TelePresence Server”			
	Task	Detailed Instructions	✓
Step 1	Configure SIP	SIP, page 3-6	
Step 2	Configure Locally Managed Mode	Locally Managed Mode, page 3-6	
Step 1	Configure the Automatic Content Handover .	Automatic Content Handover, page 3-6	
Step 2	Configure Optional Recommended Setting : <ul style="list-style-type: none"> • Display Setting 	Display Setting, page 3-7	

Cisco Video Communications Server

Table 2-4 Checklist — Configuring Cisco WebEx Enabled TelePresence on Cisco Unified CM for the First Time

Go to: Chapter 4, “Configuring Call Control”			
	Task	Detailed Instructions	✓
Step 1	Create a New DNS Zone on VCS Expressway for WebEx <ul style="list-style-type: none"> • 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 	Creating a New DNS Zone on VCS Expressway for WebEx, page 4-3	
Step 2	Configure a valid Client/Server Certificate	Configuring Certificates on Cisco VCS Expressway, page 5-1,	
Step 3	Configuring Traversal Zones for MCUs with Encryption Enabled	Configuring Traversal Zones for MCUs with Encryption Enabled, page 4-4	
Step 4	(If deploying with Unified CM) Configure a SIP trunk between Unified CM and VCS Control.	Configuring a SIP Trunk Between Unified CM and VCS Control, page 4-5	

Cisco Unified Communications Manager

Table 2-5 Checklist — Configuring Cisco WebEx Enabled TelePresence on Cisco Unified CM for the First Time

Go to: Chapter 4, "Configuring Call Control"			
	Task	Detailed Instructions	
Step 1	Configure a SIP trunk between Unified CM and VCS Control.	Configuring a SIP Trunk Between Unified CM and VCS Control, page 4-5	✓

Cisco TelePresence Management Suite

Table 2-6 Checklist — Configuring Cisco WebEx Enabled TelePresence on Cisco TMS for the First Time

Go to: Chapter 6, "Configuring Cisco TelePresence Management Suite"			
	Task	Detailed Instructions	✓
Step 1	Enable the WebEx feature in Cisco TMS.	Configuring the Cisco WebEx Feature in Cisco TMS, page 6-2	
Step 2	Configure WebEx users in Cisco TMS.	Configuring WebEx Users in Cisco TMS, page 6-4	
Step 3	Configure Hybrid Content Mode for MCU in Cisco TMS.	Configuring Hybrid Content Mode for MCU in Cisco TMS, page 6-8	

Cisco TelePresence Management Suite Extension for Microsoft Exchange

Complete the steps below if you want to deploy the feature of scheduling WebEx Enabled TelePresence meetings using the 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 2-7 Checklist – Configuring Cisco WebEx Enabled TelePresence on Cisco TMSXE for the First Time

Go to: Chapter 7, "Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange"			
	Task	Detailed Instructions	✓
Step 1	Configure TMSXE for scheduling with WebEx and TelePresence Integration to Microsoft Outlook.	Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook, page 7-2	
Step 2	Configure TMSXE for scheduling with WebEx Scheduling Mailbox.	Configuring Cisco TMSXE for the WebEx Scheduling Mailbox, page 7-6	

Cisco TelePresence Management Suite Provisioning Extension

Complete the steps below if you want to deploy the feature of scheduling Cisco WebEx Enabled TelePresence meetings using Smart Scheduler.

Table 2-8 Checklist — Configuring Cisco WebEx Enabled TelePresence on Cisco TMSPE for the First Time

	Task	Detailed Instructions	✓
Step 1	Install and enable TelePresence Management Suite Provisioning Extension (TMSPE) on TMS.	Cisco TelePresence Management Suite Provisioning Extension Deployment Guide.	
Step 2	Review additional prerequisites, and information about TMSPE and Smart Scheduler.	Configuring Cisco TelePresence Management Suite Provisioning Extension, page 8-1	

Configure Audio for Cisco WebEx Enabled TelePresence


Table 2-9 Checklist — Configuring Audio for Cisco WebEx Enabled TelePresence

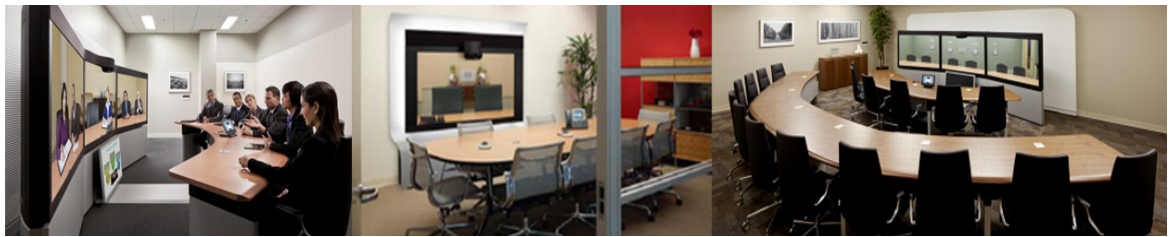
Go to: Chapter 9, "Configuring Audio"			
	Task	Detailed Instructions	✓
Step 1	Configuring SIP Audio for Cisco WebEx Enabled TelePresence: <ul style="list-style-type: none"> • Configure the WebEx Site in Cisco TMS to Use SIP Audio • Enable Hybrid Mode on the WebEx Site 	Configuring SIP Audio for Cisco WebEx Enabled TelePresence, page 9-2	
Step 2	Configuring PSTN Audio for Cisco WebEx Enabled TelePresence: <ul style="list-style-type: none"> • 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 Cisco WebEx Enabled TelePresence, page 9-3	
Step 3	(If applicable) Configuring TSP Audio for Cisco WebEx Enabled TelePresence: <ul style="list-style-type: none"> • Configure MACC Domain Index and Open TSP Meeting Room WebEx Settings • Configure TSP Dial String • Configure How the Conference is Opened • Configure TSP Audio for the Meeting Organizer 	Configuring TSP Audio for Cisco WebEx Enabled TelePresence, page 9-7	

Cisco WebEx Site Administration

After WebEx provisions your site for WebEx Enabled TelePresence, follow these steps.

Table 2-10 Checklist — Setting up Cisco WebEx Site Administration for the First Time

Go to: Chapter 10, "Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account"			
	Task	Detailed Instructions	
Step 1	Enable Cisco TelePresence Integration (MC only).	Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account	
Step 2	(Recommended) Enable TelePresence options: <ul style="list-style-type: none"> • List TelePresence on calendar • Send invitation email to meeting host • Display toll-free number to attendees 		
Step 3	Set the Cisco TelePresence VOIP and video connection.		
Step 4	Select the Cisco TelePresence PRO: Meeting Center TelePresence Session Type.	Assigning the Meeting Center TelePresence Session Type	



CHAPTER 3

Configuring Cisco MCU and TelePresence Server

Revised: July 2014



Note

You must be running MCU software release 4.4 or a later or TelePresence Server 3.0 or later to use Cisco WebEx Enabled TelePresence features.

Contents

This chapter describes how to configure MCU and TelePresence Server for Cisco WebEx Enabled TelePresence meetings. It contains the following sections:

- [Required Settings for MCU, page 3-2](#)
- [Recommended Settings for MCU, page 3-3](#)
- [Required Settings for TelePresence Server, page 3-5](#)
- [Recommended Settings for TelePresence Server, page 3-7](#)

Introduction

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

In terms of deployment, both MCU and TelePresence Server must be registered to VCS directly and cannot be trunked to Unified CM.

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 WebEx Enabled TelePresence.

Required Settings for MCU

The following settings on MCU are required for Cisco WebEx Enabled TelePresence:

- [SIP, page 3-2](#)
- [Content Mode, page 3-2](#)
- [Video and Audio Codecs, page 3-2](#)
- [Automatic Content Handover, page 3-3](#)

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

http://www.cisco.com/en/US/products/ps12283/prod_release_notes_list.html

SIP

MCU calls to WebEx support SIP only. Make sure SIP is configured correctly on MCU. The call leg between MCU/TelePresence Server, VCS Control, 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, page 6-8.](#)

Video and Audio Codecs

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

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

-
- Step 1** Log into the MCU.
 - Step 2** Click **Settings**.
 - Step 3** The Settings page appears with the Conferences tab displayed.
 - Step 4** In the Advanced Settings section make sure **H.264** is checked for the following:
 - Video codecs from MCU

- Video codecs to MCU
- Step 5** In the Advanced Settings section make sure **G.711** is checked for the following:
- Audio codecs from MCU
 - Audio codecs to MCU
- Step 6** At the bottom of the page, click **Apply changes**.
-

Automatic Content Handover

This feature must be enabled for TelePresence endpoints to share during a Cisco WebEx Enabled TelePresence meeting.

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

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

Recommended Settings for MCU

For best results with Cisco WebEx Enabled TelePresence, Cisco recommends configuring the following settings in MCU:

- [Automatically Make Content Channel Important, page 3-3](#)
- [Outgoing Transcoded Codec, page 3-4](#)
- [Adaptive Gain Control, page 3-4](#)
- [Join and Leave Audio Notifications, page 3-5](#)
- [Encryption, page 3-5](#)

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:

-
- Step 1** Log into the MCU.

- Step 2** Click **Settings**.
The Settings page appears with the Conferences tab displayed.
- Step 3** In the Advanced Settings section, check **Automatically make content channel important**.
- Step 4** 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:

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

- Step 1** Log into the MCU.
- Step 2** Click **Conferences** at the top of the page.
The Conferences page appears with the Conference list tab displayed.
- Step 3** Click the **Templates** tab.
The Conference Templates page appears.
- Step 4** Click the link for **Top level**.
The Top level template configuration page appears.
- Step 5** In the Parameters section, using the Adaptive Gain Control on join menu, select **Enabled**.
- Step 6** 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 Cisco WebEx Enabled TelePresence 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:

-
- Step 1** Log into the MCU.
- Step 2** Click **Settings**.
- The Settings page appears with the Conferences tab displayed.
- Step 3** In the Conference Settings section, for Audio Notifications, uncheck **Join and leave indications**.
- Step 4** 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:

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

Required Settings for TelePresence Server

The following setting in TelePresence Server is required for Cisco WebEx Enabled TelePresence:

- [SIP, page 3-6](#)

- [Locally Managed Mode, page 3-6](#)
- [Automatic Content Handover, page 3-6](#)

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



Note

TelePresence Server release 3.1 with a Third-Party Interop key is required for support of TSP audio.

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:

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

Automatic Content Handover

This feature must be enabled for TelePresence endpoints to share during a Cisco WebEx Enabled TelePresence meeting.

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

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

Recommended Settings for TelePresence Server

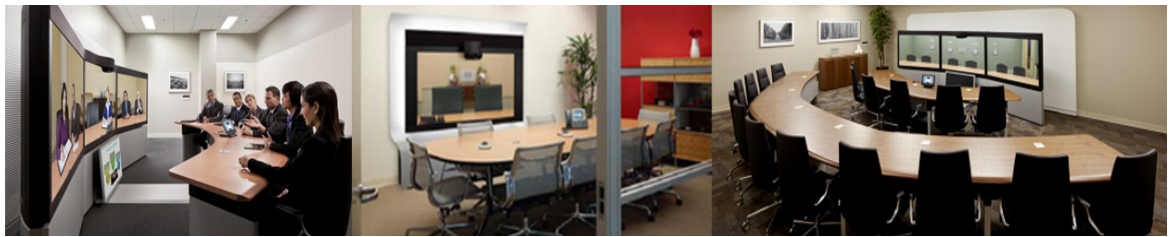
For best results with Cisco WebEx Enabled TelePresence, Cisco recommends the following settings on TelePresence Server:

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.

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

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



CHAPTER 4

Configuring Call Control

Revised: February 2014

Introduction

This chapter describes how to configure call control for Cisco WebEx Enabled TelePresence meetings. To begin using Cisco WebEx Enabled TelePresence, you must configure the call control product(s) used in your video network.

There are three possible call control scenarios:

- Cisco TelePresence VCS Control and Expressway
Endpoints are registered to VCS Control and/or Expressway only.
- Cisco Unified CM with VCS Control and Expressway
Endpoints are registered to Unified CM only.
- Cisco TelePresence VCS Control and Expressway with Unified CM
Endpoints are registered to VCS Control/Expressway and Unified CM.



Note

Using Unified CM as the call control solution requires VCS Control and Expressway to be deployed in order to communicate with WebEx, regardless of whether endpoints are registered to VCS Control and Expressway or not.

Configuring Cisco TelePresence Video Communication Server Control and Expressway

The following section describes the steps required for configuring Cisco TelePresence Video Communication Server Control and Expressway for Cisco WebEx Enabled TelePresence.

This section describes the following tasks:

- [Prerequisites, page 4-2](#)
- [Creating a New DNS Zone on VCS Expressway for WebEx, page 4-3](#)
- [Configuring Traversal Zones for MCUs with Encryption Enabled, page 4-4](#)

Prerequisites

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

- Cisco TelePresence Video Communication Server (VCS) must be running firmware X7.2.2 or a later release.
- Endpoints in the network are registered to 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 VCS Control. For more information, refer to [Configuring Cisco Unified Communications Manager, page 4-4](#).

- Expressway must be assigned a static IP address
- Firewall must have port 5061 open to allow access to Expressway
 - **If this port is not configured correctly, calls will not take place correctly.**
- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network
- VCS Control is in the private network
- 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 1.1 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

- VCS Control is configured as the SIP Registrar/H.323 gatekeeper.

In order for Cisco WebEx Enabled TelePresence to work, it is required to set up a VCS Control as a SIP registrar, enabling it to register SIP devices and route calls to them. VCS Control has the capability to be both an H.323 gatekeeper and a SIP registrar.

Configuring VCS as a SIP registrar is done by configuring one or more SIP domains. The VCS 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 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 VCS Expressway for your configured SIP Domain so TelePresence participants can route to your VCS Expressway.
-

Creating a New DNS Zone on VCS Expressway for WebEx

By default, a VCS solution will handle local domains, and route calls to non-local domains to the VCS Expressway to route them to the Internet via a DNS zone.

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

To configure the VCS Expressway for Cisco WebEx Enabled TelePresence, do the following:

-
- Step 1** Create a new DNS zone:
- Set H.323 to **Off**.
 - Set SIP Media encryption mode to **Force encrypted**.
 - Turn on TLS Verify mode.
 - In the TLS verify subject name field, enter **sip.webex.com**.
 - Click **Create Zone**.
- Step 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_C onfiguration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-1.pdf.

- Step 3** Configure a valid Client/Server Certificate for your company. Typically the CName of the certificate is the routable domain to your company’s VCS Expressway. It must be a CA-level certificate name issued by a public CA that is supported by WebEx.



Caution

Self-signed certificates are NOT supported.

For a list of supported certificates and details on how to configure a certificate on VCS Expressway, refer to: [Chapter 5, “Configuring Certificates on Cisco VCS Expressway”](#).

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).

**Caution**

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.

To support MCUs that have encryption enabled, do the following

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



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

Step 2 On VCS Expressway, set up a new traversal server zone that connects to the VCS Control traversal zone set up in the previous step.

Step 3 In this new VCS Expressway traversal server zone, set media encryption to **Force unencrypted**.

Step 4 On 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 Cisco WebEx Enabled TelePresence. This configuration also supports a deployments where endpoints are registered to Unified CM only or both Unified CM and VCS Control/Expressway.

This section describes the following tasks:

- [Prerequisites, page 4-4](#)
- [Configuring a SIP Trunk Between Unified CM and VCS Control, page 4-5](#)

Prerequisites

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

- Cisco Unified CM 8.6.2 or 9.1.1.
- Endpoints in the network are registered to Unified CM

- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network and registered to VCS
- 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 1.3 Mbps.
- VCS expressway configured with the DNS zone.

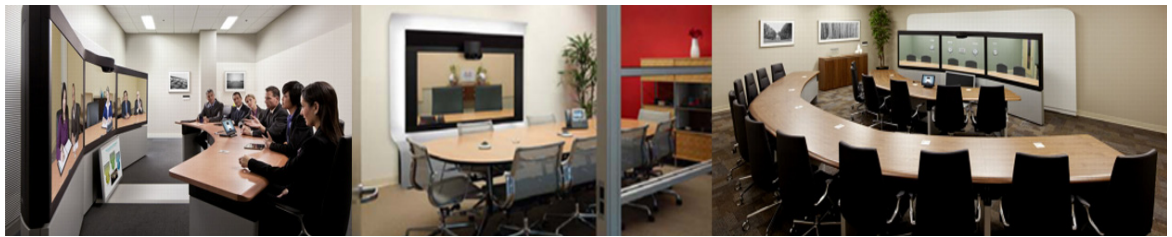
Configuring a SIP Trunk Between Unified CM and VCS Control

This section describes how to configure the Cisco TelePresence Video Communication Server (Cisco VCS) version X7.2.1 or later and Cisco Unified Communications Manager (Unified CM versions 6.1, 7 or 8 to interwork via a SIP trunk.

This is required for endpoints registered to Unified CM to participate in a Cisco WebEx Enabled TelePresence meeting and to call endpoints registered to 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 TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide at the following location:

[Cisco VCS and Unified CM Deployment Guide \(Unified CM 8.6.x, 9.x and VCS X7.2\)](#).



CHAPTER 5

Configuring Certificates on Cisco VCS Expressway

Revised: April 2014

Introduction

This chapter describes the best practices for configuring certificates on Cisco VCS Expressway.

There are three parts to the configuration:

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

Both VCS Expressway X7.2.2 and X8.1 are supported. There are important differences in how each are configured, which are noted in the procedures that follow.



Caution

Customers using Static NAT on VCS Expressway X7.2.2 are highly recommended to not upgrade to X8.1. If you are using Static NAT with X8.1, refer to the recommended workarounds in [VCS Expressway X8.1 Encryption Issue and Workarounds](#).

VCS Expressway X8.1 Encryption Issue and Workarounds

There is an issue with the Encrypt on Behalf feature in VCS Expressway X8.1 when using Static NAT. Because VCS Expressway X8.1 uses 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 X7.2.2 are urged not to upgrade to X8.1 until a maintenance release fixes this issue.

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

- Downgrade VCS Expressway to X7.2.2.
- Reconfigure VCS Expressway X8.1 to not use Static NAT.
- Use VCS Control to Encrypt on Behalf instead of VCS Expressway.

To use VCS Control to encrypt on behalf, do the following:

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

Videos Available

The entire configuration process for VCS Expressway 7.2.2 is also described and demonstrated in the following video series:

[Configuring Certificates on Cisco VCS Expressway for WebEx Enabled TelePresence](#)

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 VCS Expressway will not be authorized 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*
- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- globalsign_root_ca
- thawte_primary_root_ca
- geotrust_primary_ca

- addtrust_external_ca_root



Note This list may change over time. For the most current information, contact WebEx.

*To use a certificate generated by entrust_2048_ca with Cisco VCS Expressway, 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 at the following URL:

https://www.entrust.net/downloads/root_index.cfm



Caution

Wildcard certificates are not supported on VCS Expressway.

Generating a Certificate Signing Request (CSR)

To generate a certificate signing request, do the following:

-
- Step 1** In VCS Expressway:
- X7.2.2, go to **Maintenance > Certificate management > Server certificate**.
 - X8.1, go to **Maintenance > Security certificates > Server certificate**.
- Step 2** Click **Generate CSR**.

■ Generating a Certificate Signing Request (CSR)

CISCO Cisco TelePresence Video Communication Server Expressway

Status **System** VCS configuration Applications **Maintenance** [? Help](#) [Logout](#)

Server certificate You are here: [Maintenance](#) > [Certificate management](#) > Server certificate

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	There is no certificate signing request in progress
---------------------	---

Generate CSR

Upload new certificate

Select the server private key file	<input type="text"/>	Browse...	i
Select the server certificate file	<input type="text"/>	Browse...	i

[Upload server certificate data](#)

Generate CSR You are here: [Maintenance](#) > [Certif](#)

Generate Certificate Signing Request

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

Generate CSR

Step 3 Enter the required information for the CSR and click **Generate CSR**.

After clicking the Generate CSR button, the Server Certificate page is displayed and 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, this will force you to regenerate the CSR and the auto-generated private key will not appear on the Server Certificate page.

Generating a Certificate Signing Request (CSR)

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...](#) [i](#)

[Upload server certificate data](#)

Step 4 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](#) > [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

[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-----
MIIDLDCCAhQCAQAwEjEhMB8GA1UEAwYY3RnLWVmdC12Y3NlLlTEuY2lZy28uY29t
MQswCQYDVQQGEwJWUzETMBEGA1UECAwKQ2FsaWZvcn5yTERMA8GA1UEBwwIU2Fu
IEpvc2UxXjAMBGNVBAoMBUNpc2NvMRAwDgYDVQQLEAdVcG9uRUZUMiI1IjANBgkq
hkIG9w0BAQEFAAOCQAQ8AMIIBCgKCAQEAuqf35MXVBYnZyXbsKDbY+ZEXPDH4fqt4
fULpqtBEbD/z148dib7/i+UmMIS0RN9deXatSTtkZ7vh3VghvRfGzy63t2wu6FHy
bmkMxBu82UhnfmPHC3WtpFZKoG95hWi0jR66yWE43ZqkeYBUkn9Ij7hKD+YyTbMA
3JnzF8cEGh8KEK5RjfbBbRqVwep1wXT0N92Y8tm3hitnHGhzFEvXk7qZNeEAIx9Dv
e69PqjdiB0RvSNk7GrLQRg5u0RvUgPjHBLug9H0Y1MMQeK6xvrgEfLACgn/i55rT
Sy6eEbiZfmrNHNf+/zIr7utphlzhliYZAV5zaxXBCbbmOvs0RNYB0wIDAQABoG0w
awYJKoZIhvcNAQkOMV4wXDAJBGNVHRMEAjAAMAsGA1UdDwQEAwIF4DAdBgNVHSUE
FjAUBgggrBgEFBQcDAQYIKwYBBQUHwIwIwYDVR0RBwwGoIYY3RnLWVmdC12Y3Nl
LlTEuY2lZy28uY29tMA0GCsqSIB3DQEBBAUAA4IBAQBmquN74IDxgb5PvyPT3oYM
hYwiUxYso+900kqyJbzM5i5g+GKMQRcy70rb5EEQt3RyD2Qyzt4jsAu6rpSrqlJ
mc1J/jJspIEL1EXtgo69T47aGhYxoG0xd7neMUT3p5qG5w7cWaxiMEzRfBj16MBH
RaBgPNDsIkzbaQt2Md0W13no0ux0ZCV//KsKOMKdwm1kYkp+Noqw05hYToKEAGgf
ijgEemDeHw5HxwL8XmpfvsTJ3Z86DiRzbvLHpNnuXVQuzF48DsD+rIjkcM90YRj
R4W4e12+vuYQ/oDRHKK1UQm3v4IfociI04dMjRdI3m6NPKsmKvh5fKxgtz26Hf4g
-----END CERTIFICATE REQUEST-----
```

Step 5 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've received the SSL server certificate from your public CA, you are ready to install it on the VCS Expressway.

Installing the SSL Server Certificate on the VCS Expressway

Note

Before installing the server certificate on the 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 VCS Expressway, do the following:

- Step 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).

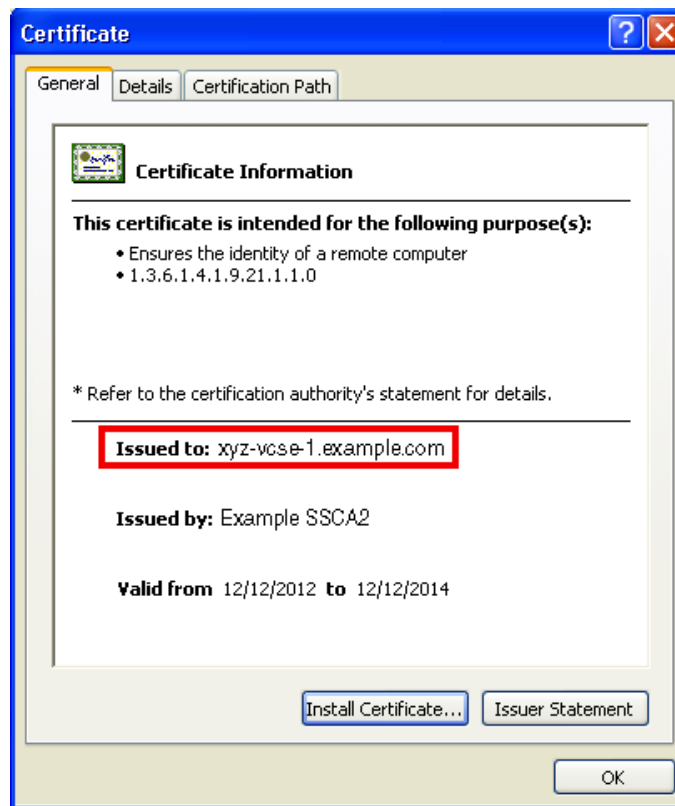


```

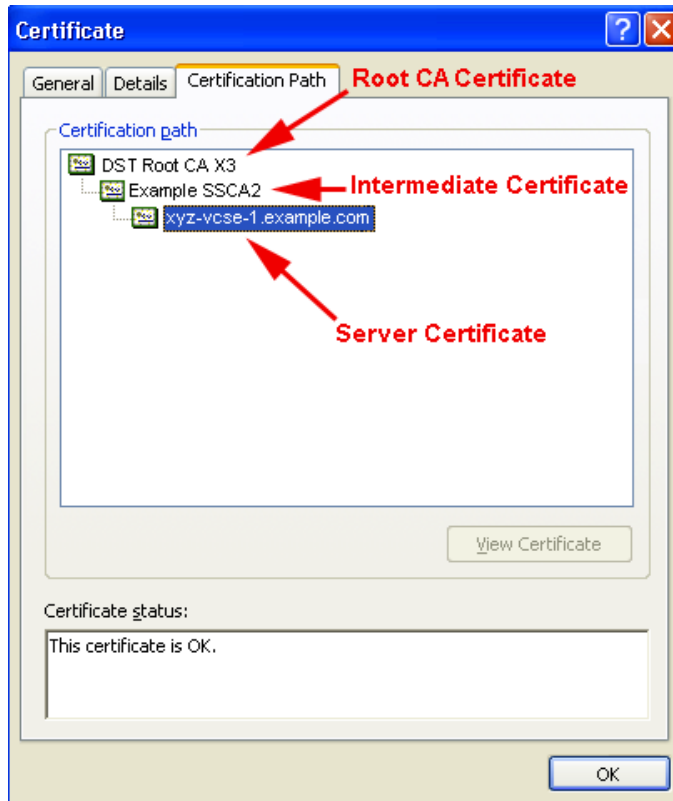
server.cer - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIIE3jCCA8agAwIBAgIKLA/ZRwAAAAAM/zANBgkqhkiG9w0BAQUFADAUMRYwFAYD
VQQKEw1DaXNjbyBTZXN0ZW1zMRRQWEGYDVQQDEwtDaXNjbyBTU0NBMTAeFw0xMjE5
MTIxODIyMTBaFw0xNDYyMTIxODMyMTBaMHoxCzAJBgNVBAYTA1VTMRMwEQYDVQQL
EwpDYWxwZm9ybmlhMREwDwYDVQQHEWhTYW4gSm9zZTEOMAwGA1UEChMFQ21yZ28x
EDA0BgNVBAsTB0NURyBFRlQxITAFBgNVBAMTGGN0Zy11Znqt dmnZZ50xLmNpc2Nv
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+FGolui02+U0sd
6DQjSR0ddvW9RZEdGxxl0pVSR1caIr lFM72NbJGH/ot/3pq5kjHtKzKAQYD12gw
ZPPbh3+YGOy0gKEjzx17yrXNXnoDux5LSJNBP0ppXGFTi5pAZuHrX414wpub0B
dJXMGsazw9Pwf78FQWJoetCS7GK9w6nIZGcEN3kAOR7Mm5xyvCM5dg2GHF+w2Q9o
IIWtW3Q+PD128/4uwySJq01wRm0TqupzeDvVzcc5/i01F975oNnuxQz/H//Os0vF
aqYohUGJTCWgubH7qqARxv+8f3Ltpw6x52wkYMYgmoy1aIOVne6B9fK7m0azMFSq
tFcedCsCAwEAAaOCAbAwggGSMawGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgXgMDSG
A1UdJQ0MDIGCCSGAQUFBwMBBggrBgEFBQcDAGYIKWYBBQUHAWUGCCSGAQUFBwMG
BggrBgEFBQcDBZAJBgNVHREEHDAaghhjdGctZwZ0LXZjc2UtMS5jaXNjby5jb20w
HQYDVR00BBYEFPbtwZxojYRqmc00NSC0Tc5UnB+YMB8GA1UdIwQYMBaAFMewEAQv
8BfhF5BKsyphqgtXX6S7MEAGA1UdHwQ5MDcwnaAzodGGL2h0dHA6Ly93d3cuY21y
Y28uY29tL3N1Y3VyaxR5L3Bras9jcmwvc3NjYTIuY3JSMEOGCCSGAQUFBwEBBEEW
PZA9BggrBgEFBQcCwAqYxaHR0cdovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvZGtP
L2N1cnRlZ3NzY2EyLmN1c2N1c2N1c2N1c2N1c2N1c2N1c2N1c2N1c2N1c2N1c2N1c2
aWVzL2luzGV4Lmho0bwwdQYJKoZIhvcNAQEFBQADggEBALaFCDjvZjwx8j2gb4ac
ebJ0b5tov2+u1I1ldwf9+d4/u0jIDnyosn6TfdzIDRYEzC75s3lbe1SFEX+c2ohy1
VHVie8A841SSBBD0n4xq2VcmGr+jpavhncPyAevlXvtC4wxorfVOR/Nug5r19ov
/V5Kcj5NgDxBbeApwTGSJm1mx4lpzAY01Nw00j4osw3s9l6j1vyr9a4qUR+ZKoeO
lMyP6XsyCBXUXvH7zp0ltgh93M1oveq3TnsG7404ITSCDPuXPFBE2LwzjJdcJN45
9MJqq0aM5jGR74bbHcq65gnokukRZPrmz7eFQpc342kca5dP9QEHjuf839rcd7p
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 VCS Expressway server.

**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.



Step 2 In VCS Expressway:

- X7.2.2, Go to **Maintenance > Certificate management > Server certificate**.
- X8.1, Go to **Maintenance > Security certificates > Server certificate**.

Step 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.

Step 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	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	<input type="text"/>	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	Show server certificate
Currently loaded certificate expires on	Dec 12 2014	


[Reset to default server certificate](#)


Certificate signing request (CSR)

Certificate request There is no certificate signing request in progress

[Generate CSR](#)

Upload new certificate

Select the server private key file [Browse...](#) 

Select the server certificate file [Browse...](#) 

[Upload server certificate data](#)

Configuring the Trusted CA Certificate List on the VCS Expressway

The version of VCS Expressway you are using will determine how you configure the trusted CA certificate list.

VCS Expressway X7.2.2

The default trusted CA certificate list for VCS Expressway X7.2.2 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 VCS Expressway X7.2.2, go to [Configuring the Trusted CA Certificate List on VCS Expressway X7.2.2](#).

VCS Expressway Upgraded from X7.2.2 to X8.1

If you upgraded your VCS Expressway from X7.2.2 to X8.1, the trusted CA certificate list from X7.2.2 will be retained.

For details on how to configure the trusted CA certificate list on VCS Expressway upgraded from X7.2.2 to X8.1, go to [Configuring the Trusted CA Certificate List on VCS Expressway Upgraded from X7.2.2 to X8.1](#).

VCS Expressway X8.1

If you are using a freshly installed 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 VCS Expressway, which is DST Root CA X3.

For details on how to configure the trusted CA certificate list on a freshly installed VCS Expressway X8.1, go to [Configuring the Trusted CA Certificate List on VCS Expressway X8.1](#).

Configuring the Trusted CA Certificate List on VCS Expressway X7.2.2

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

Resetting the Trusted CA Certificate List on VCS Expressway X7.2.2

To reset the trusted CA certificate list on VCS Expressway X7.2.2, do the following:

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



Note

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

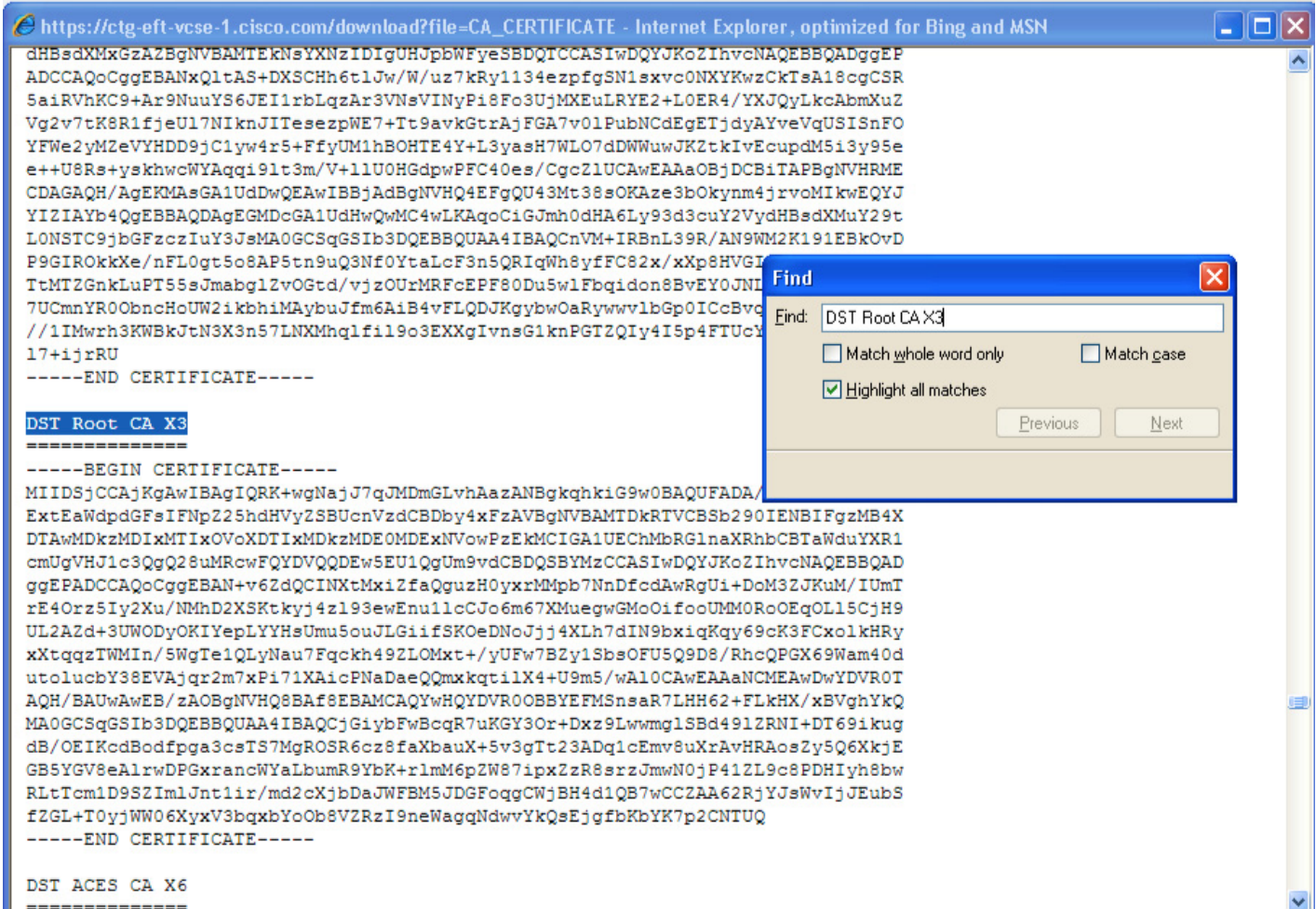
The default trusted CA certificate list on the VCS Expressway already contains the public root CA Certificate for the server certificate that the cloud will present. The root CA for the WebEx cloud is DST Root CA X3 with an intermediate CA of Cisco SSCA2.

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.

- Step 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 VCS Expressway.

- Step 3** Search for the root CA that issued the server certificate.



```

https://ctg-eft-vcse-1.cisco.com/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN
dHBsdXXmGzAZBqNVBAMTEKRNsYXNzIDIGUHJpbWFyeSBdQTCCASiWdQYJKoZlInvcNAQEBBQADggEP
ADCCAQoCggEBANxQltAS+DXSCHh6t1Jw/W/uz7kRy1134ezpfgSN1sxvc0NXyKwzCkTtA18cgCSR
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsvINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeU17NIknJITesezpwE7+Tt9avkGtrAjFGA7v01PubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWwWJK2tkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqq19lt3m/V+11U0HGdpwPFC40es/CgcZ1UCAwEAAaOjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsgA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvvoMIkwEQYJ
YI2IAyb4QgEBBAQDAGEMDcGA1UdHwQwMC4wLKAqoCIGJmh0dHA6Ly93d3cuY2VydHBEdXMmuY29t
LONSTC9jbgGFzcZiY3JmSA0GCSqGSIB3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkkXe/nFL0gt5o8AP5tn9uQ3NF0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVGIT
TtMtZGnkLuPT55sJmaq1Zv0Gtd/vjzOUrMRFcEPF80Du5w1Fbqidon8BvEY0JN1
7UCmnYR0ObncHoUW2ikbhiMAYbuJfm6A1B4vFLQDJKgybwOaRywwv1bGp0ICcBvc
//1IMwrh3KWBkJtN3X3n57LNXMhqlf1l9o3EXXgIvnsG1knPGT2QIy4I5p4FTUcY
17+ijrRU
-----END CERTIFICATE-----

DST Root CA X3
=====
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKqAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDbY4xFzAVBgNVBAMTDkRTVCBsb290IENBI FgzMB4X
DTAwMDkzMDEiXMTIxOVoXDTIxMDkzMDEOMDExNVowPzEkMCIgA1UEChMhRGlNaXRhbCBTaWduYXR1
cmUgVHJlc3QgQ28uMRcwFQYDVOQDEw5EU1QgUm9vdCBDQSBYmZCCASiWdQYJKoZlInvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdGcINXtMxi2faQguzH0yxrMMpb7NndfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSktkyj4z193ewEnu1lcCJo6m67XMuegwGMOoIfoUUM0RoOEQOL15CjH9
UL2AZd+3UWODyOKIYepLYYHsUmuSouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRy
xXtqzqTWMIn/5WgTe1QLyNau7FqcKh49ZLOMxt+/yUfW7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utocluchY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtl1X4+U9m5/wAl0CAwEAAANCMEEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBvghYkQ
MA0GCSqGSIB3DQEBBQUAA4IBAQCjG1ybFwBcqR7uKGY3Or+Dxz9Lwmmg1SBd491ZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSr6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAos2y5Q6XkjE
GB5YGV8eAlrwdPGxranwYaLbumR9YbK+r1mM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9S2ImlJnt1ir/md2cXjbDaJWFbM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJswVrIJEubS
fZGL+I0yJWW06XyxV3bqxbyoOb8VZRzI9neWagqNdwwYkQsEjgfbKbYK7p2CNTUQ
-----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 your VCS Expressway is complete.

If the server certificate is issued by an intermediate CA, go to the next section.



Note

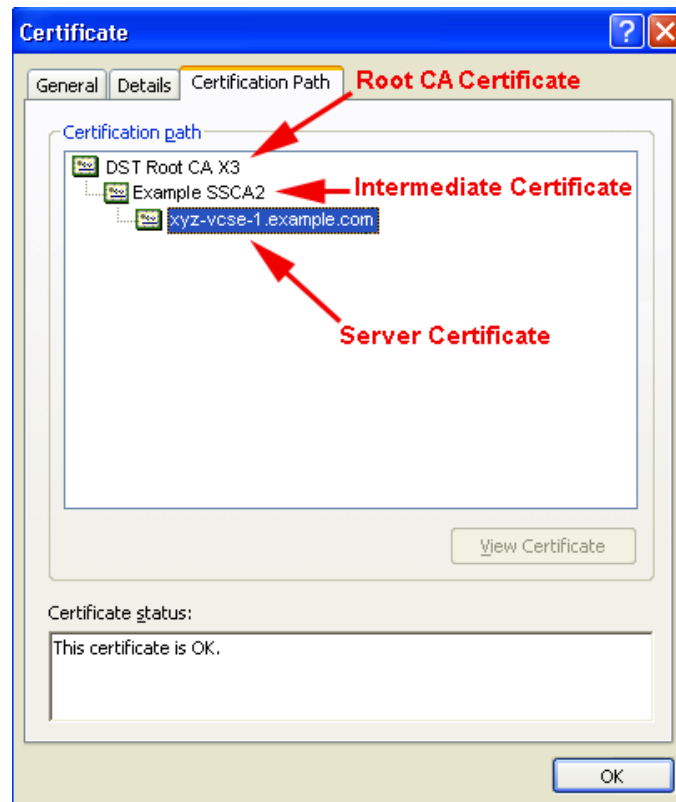
If the certificate for the top-level root CA that issued your server certificate is not part of the default trusted CA certificate list, you must add it using the same procedure that is described for stacking the intermediate CA certificate, detailed in the next section.

Stacking the Intermediate CA Certificate in the Trusted CA Certificate List on VCS Expressway X7.2.2

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

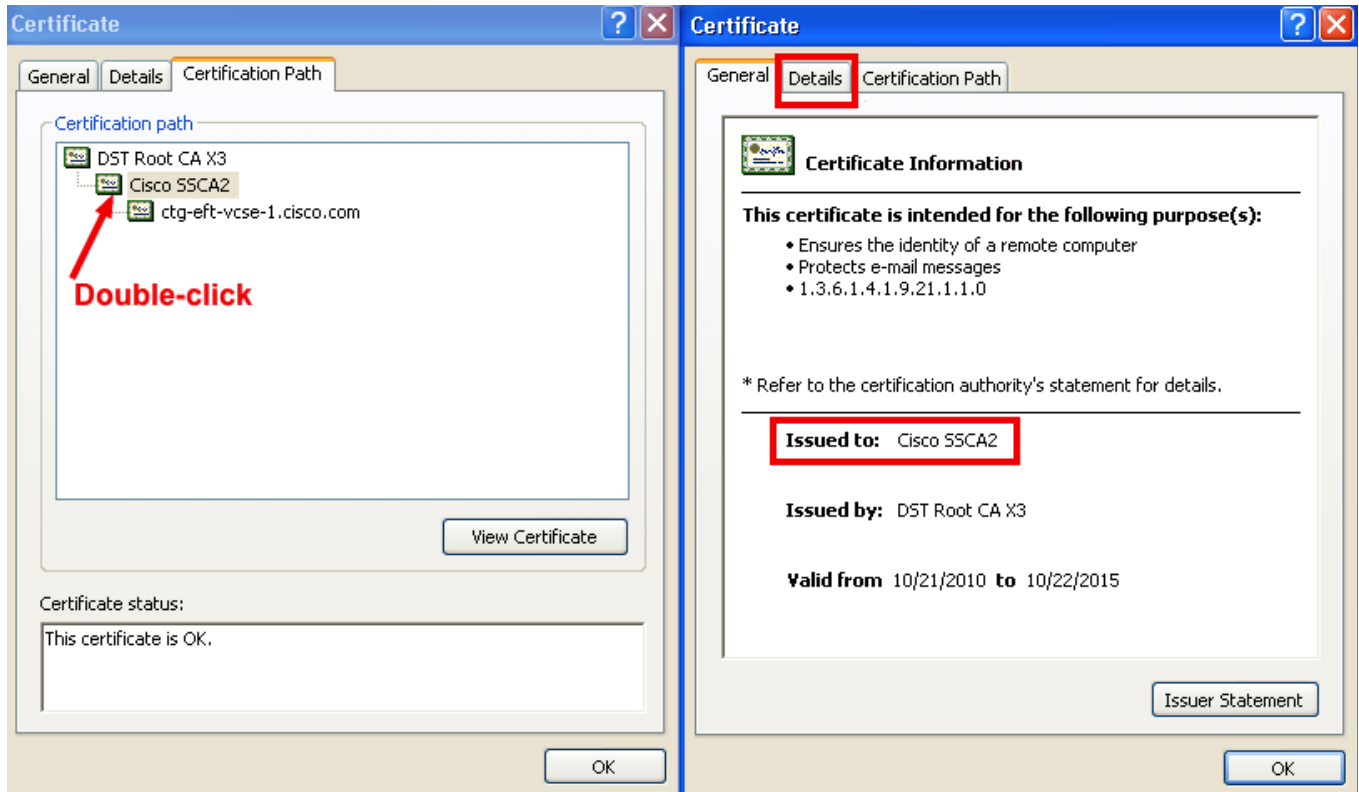
If the server certificate is issued by an intermediate CA, then you'll need to add the intermediate CA certificate to the default Trusted CA list.

Figure 5-1 Server Certificate in .CER File Format



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're that you're stacking the correct intermediate CA certificate.

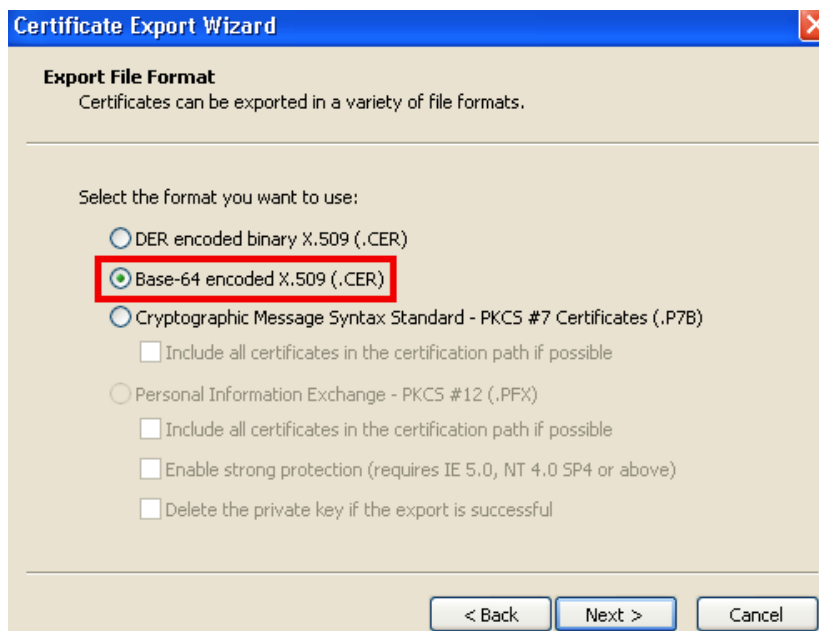
-
- Step 1** Open the server certificate as a .CER file (see [Figure 5-1](#))
 - Step 2** Click the **Certification Path** tab, double-click the **Intermediate Certificate**.
This will open the intermediate CA certificate in a separate certificate viewer.
 - Step 3** Make sure the 'Issued to' field displays the name of the Intermediate CA.
 - Step 4** Click the **Details** tab followed by **Copy to File...**



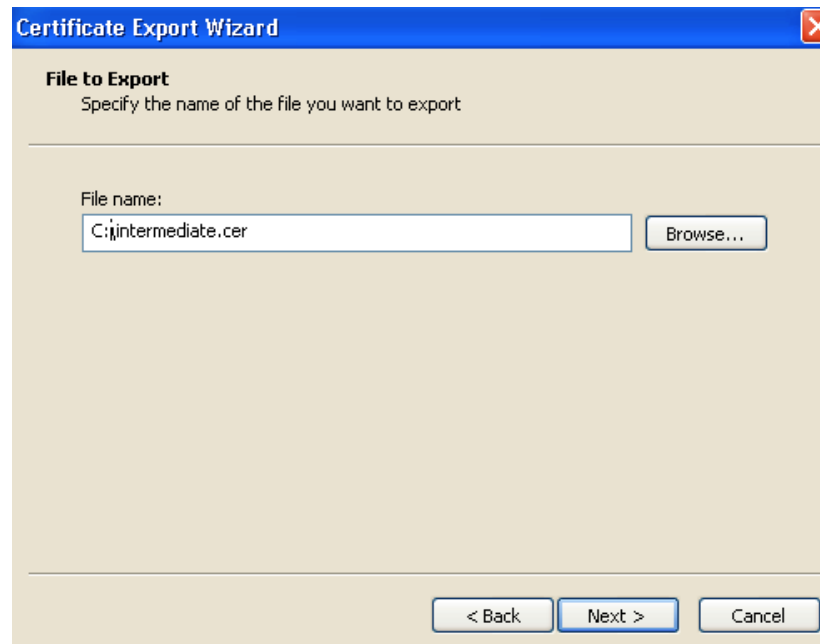
The 'Welcome to the Certificate Export Wizard' appears.

Step 5 Click **Next**.

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



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



- Step 8** Copy the default Trusted CA list from the VCS Expressway by going to **Maintenance > Certificate management > Trusted CA certificate** and clicking **Show CA Certificate**. In the window that opens, select all contents.
- Step 9** Paste the contents into a text editing application such as Notepad.
- Step 10** Open the intermediate.cer file within a new window of your text editing application and copy the contents to your clipboard.
- Step 11** Do a search for the existing root CA certificate within the text file that contains the contents of the default Trusted CA list.
- Step 12** Paste the intermediate CA certificate above the root certificate.
- Step 13** Save the text file as .PEM file (Example: *NewDefaultCA.pem*)

Configuring the Trusted CA Certificate List on the VCS Expressway

```

ca.txt - Notepad
File Edit Format View Help
ADCCAQCggEBANxQ1tAS+DXSCHh6t1Jw/w/uz7kry1134ezpfgSNLSxvc0NXyKwzCkTsA18cgCSR
5a1rVhKc9+Ar9NuUyS6JE1rblqzAr3VnSVINyP18Fo3UjMxkEULRYE2+L0ER4/yxJQyLkCabmxuz
Vg2v7tK8R1fjEul7NiknJITesEzPwE7+Tt9avkGtRajFGA7v01PubncDEgetjdyAYvevquSInFO
YFWe2YMzeVYHDD9jClyw4r5+FFyUM1hBOHE4Y+L3yasH7WLO7dWwUwJKZtkIvEcupdm513y95e
e++U8R+s+yshwcyAqq191t3m/V+11U0HGdpwPFC40es/CgcZ1UCAwEAAaObjDCb1tAPBgNVHRME
CDAGAQH/AgEKMASGALUdWQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAzE3bokynm4jrvomIkweQYJ
YIZIAYb4QgEBBAQDAgEMDCA1UdHwQwM4WLKAQoc1Gjmh0dHA6Ly93d3cuY2VydyHBSdxMuy29t
L0NST9jbgfzcziuy3JSMaQGSqSgSiB3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9wM2K191EBkOvd
P9GIrokKxe/nFL0gt5o8AP5tn9uQ3NF0YtalCF3n5QRiQwh8YffC82x/xxp8HVGIutIKP1dd311R
TtMTZgnkLUPT55sJmabg1zvOGtd/vj2ouMRrCEPF80Du5w1Fbq1don8BvEY0JNLdnyct6X091/+
7UCmnyR00bnchoUw21k6h1MaybuJfm6A1B4vFLQDJkybwoaRywwv1bGp0IccBvqQN16BQNwB6Sw
//1Imwrh3kwbKJtN3x3n57LNXmhlfi19o3EXxgIvnsG1knpGTZQy4I5p4FTUCy1Rbpsda2ENw7
17+1jrRU
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIFB2CCA++gAwIBAgIQcGFBQgAAASVQQLRnAAAAAJANBgkqhkiG9w0BAQUFADA/
MSQwIydvQKExtEawdpdGFsIFNpZ25hdHvyZSBucnVzdCBDbY4xFzAVBgNVBAMTDkRtVCBsb290IENBIFg2MB4XD
LjEwMDQ0GALUECHMhQ21y28gu31zdGvtczEUMBIGALUEAXMLQ21y28gu1NDQTIw
ggE1MA0GCSqS5Ib3DQEBBAQUAAIBDwAwgEKAAoIBAQRDR8snf0EhLuvvehkf1ToCJ
xGknpp/66fqx35tpgqjgm420P+oIB21H9vyAHwIY5eGJELYH5zC8o1sdjqua2qt4
bv5bgVLB+aoFka1mFFZifmtJjcuqwj1t8d2OD2IOvUN6k9LJepssdqEUScsEgPpz
CXouYfVK2A1Z1YfB6wNHT1eAab8Mcdtn0j3593uxXLHqdtSPP11tJdnPoswF1yxs
3t7n3MesugxtSuiT59sbSuo6+cyfsD6EnIagFHokrE6MMgEvNkxr4IQLVsc87y
k98n5yA8EAycgp5X19pl86cwrwoj23xGunkNouIymudawhcmeyDP2XI07XypgLER
AQmBAAGjggIOMIICCjAObgNVHQ8BAF8EBAMCAAYwEgYDVR0TAQH/BAgwBgEB/wIB
ADBCBQNVHSAEVTBTMFEgc1sGAQQBRCUBAQAQZBBBggRgBGFBCQARY1AHR0CDOV
L3d3dy5jxNjby5j2b0vc2vjdx3pdhkvCGtPL3Bvb51jawnzL21uzGv4Lmh0bww
HQYDVR00BBYEFmewEAgv8BhFh5Bksyphqgtxx657MDkGALUdHwQwMDAwLQAsocGg
KGh0dHA6Ly9jcmwuaWR1bnRydXN0LmNvb59EU1RST09UQ0FYMy5jcmwudAYIKwYB
BQUHAQEEDBMMCCGCSGAQUFBzABhhtodHRwo18vb2NzCHRzLm1kZw50cnVzdC5j
b20wOwYIKwYBBQUHMAKGL2h0dHA6Ly9hCHBzLm1kZw50cnVzdC5j2b0vc9m9dHVM
RfNUUK9PVENBWDUMY2YyMIgUBGNVHSUEgywgykGCCSQAQUFBwMBBggRgBGFBCD
AgYIKwYBBQUHAWMGCSGAQUFBwMBBggRgBGFBCDBQYIKwYBBQUHAWYGCCSQAQUF
BwMHBggRgBGFBCQCAyIKwYBBQUHAWKGC1sGAQQBgjckAwEGC1sGAQQBgjckAwkG
C1sGAQQBgjckAwEGC5sGAQQBgjcvb1AfBgNVHSMEGDAwBTEp7Gkyxx+tvhs5B1
/8QVY1WjEDANBgkqhkiG9w0BAQUFAAoCAQEAvrBuxbGT4vxdwhrj+oejP/8ckyB
gg5G+2V07o2MPTvuyTMEfz2v3k2mXAXF461MYvY5xw8NdPaxctP/Q5xdQN1XTn40
YsnWhXHLCCAFa7/MOKNICY0FL4Bnop0w8fdtigh19rMaoww4ycExvYrXm5HjrCh
FG4NdrYuyw1TtAGLZ6j6vMuAT1JP10qmaoRj8NngA9Act87oLmx1qt+ev1qu1FT
3v14odHz1Y3WZUR7grQawEYfQHEUj2A0GRHlmcJ1CFfLCSZjCSKSOxbgnfna8z
5nIbIZIwXfSuxXDOELhmZJY1dmuqYxkTQohrtLwktk5fk1zGJpmezuzg==
-----END CERTIFICATE-----

DST Root CA X3
-----BEGIN CERTIFICATE-----
MIIDSjCCA1kgAwIBAgIQQRk+wgnaJj7JQMDmGLvhaazANBgkqhkiG9w0BAQUFADA/MSQwIydvQKExtEawdpdGFsIFNpZ25hdHvyZSBucnVzdCBDbY4xFzAVBgNVBAMTDkRtVCBsb290IENBIFg2MB4XD
DTAwMDkzMDI1MTI1xOVXDTIxMDkzMDU0MDExNvowPzEkMCIGA1UECHMBrG1naXRhcCBTawduYXR1cmUgVHJ1c3QgQ28URmFQYDQVQDEw5EU1Qgum9vdcBDQSBYmZCCAS1wDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQCINxtMx1zfAqguzH0yxrMMpb7NndfcdAwRgui+doM3ZJKUM/IUMT
rE4or25IY2xu/NMhd2XSktkyj4z193ewenu1ccJo6m67xmuegwmoo1foouMM0Ro0eQOL15cjH9
UL2AZd+3UwodyOKIYepLYHsUm5ouJLGI1fSKoEDNOj14XL7dIN9bx1qkqy69ck3FCx01kHRY
XXtqqzTWMIIn/5wgTE1QLyNau7Fqckh49ZL0Mxt+/yUfW7Bzy1SbsOFU5Q9D8/RhcQPGX69Wam40d
ut0Lucby38EvaJqr2m7xPi71XA1cPNaDaeeqQmxkqt1X4+U9m5/wa10CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/ZAObgNVHQ8BAF8EBAMCAQYWHQYDVR00BBYEFMSnsar7LHH62+FLkHX/xBVghyKQ
MA0GCSqS5Ib3DQEBBQUAA4IBAQCjG1ybFwBcqR7UKGY3Or+Dx29Lwmg1SBd491ZRNI+DT691kug
dB/OEIKcdBdfpga3csTS7MgROSR6cz8FAXBauX+5v3gTt23ADQ1cEmv8uXrAvHRAos2Y5Q6XkjE
GB5YGV8eA1rWDPGxrancwYALbumr9Ybk+r1m6pZw871pxzZR8srzJmwn0jP41ZL9c8PDHIyh8bw
RLTclm1D9SZIm1Jnt11r/md2cx1bdaJwFBM5JDFGogqCwjBH4d1QB7wCCZAA62RjYJswW1jJEubs
fZGL+T0yJw06xyv3bqxbYooB8VZRZ19newagqndwYkQsEjgfbkBYK7p2CNTUq
-----END CERTIFICATE-----

DST ACES CA X6
-----BEGIN CERTIFICATE-----
MIIECTCAvGgAwIBAgIQDv6ZCtadt3js2Adwo4Yv2TANBgkqhkiG9w0BAQUFAADBMQswCQYDVQQG
EwJVUzEgMB4GALUECFMxRG1naXRhcCBTawduYXR1cmUgVHJ1c3QxETAPBgNVBAsTCERTVCBBQ0VT

```

Pasted Intermediate CA Certificate

Existing Root CA Certificate

Note

If the root CA is not part of the default trusted CA list. Follow same procedure of stacking the intermediate CA certificate.

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

Step 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 ⓘ

CA certificate

Certificate configuration on your VCS Expressway X7.2.2 is complete.

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to the “Cisco VCS Certificate Creation and Use Deployment Guide (X7.2)” 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 VCS Expressway Upgraded from X7.2.2 to X8.1

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

Resetting the Trusted CA Certificate List on VCS Expressway Upgraded from X7.2.2. to X8.1

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

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



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

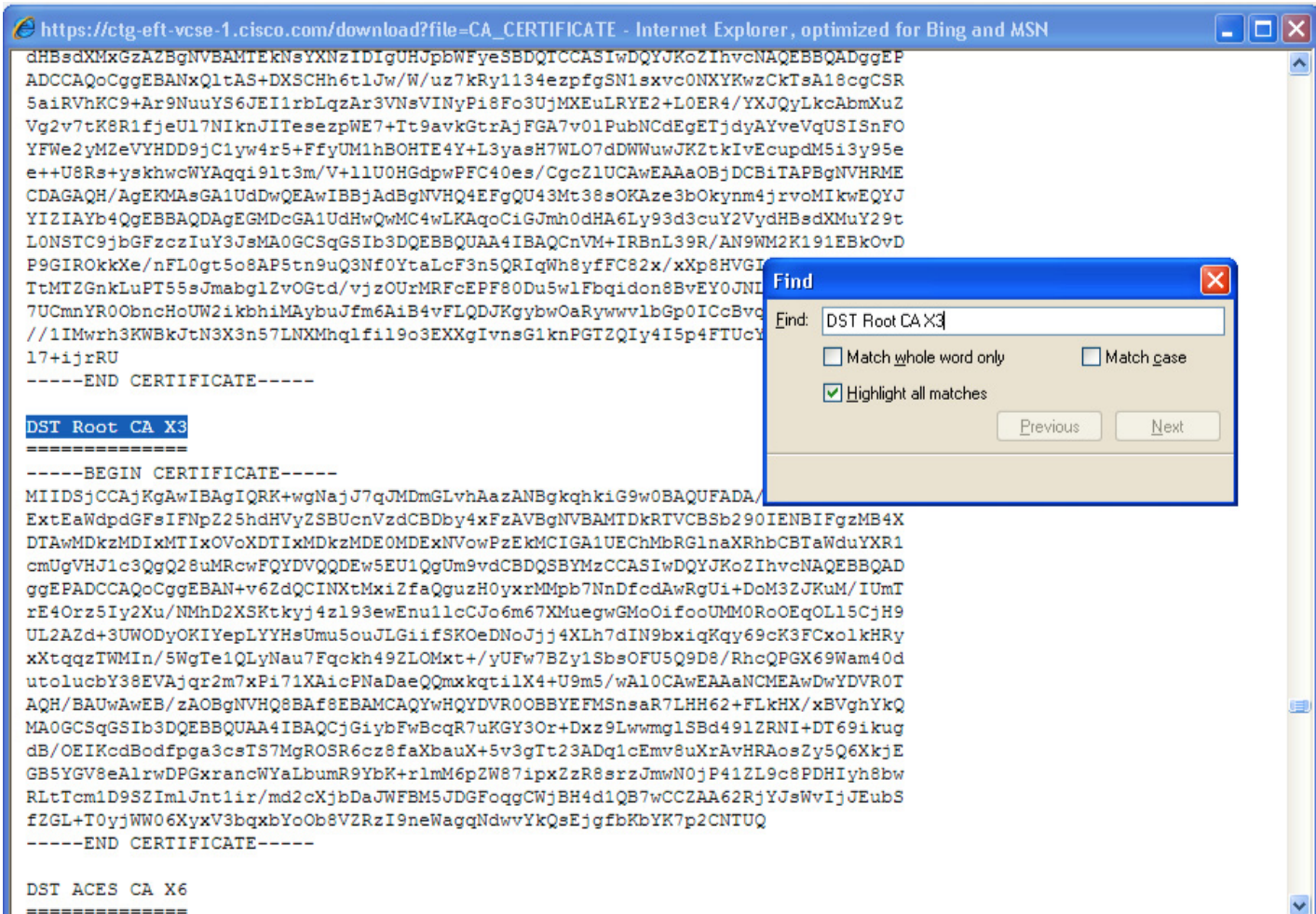
The default trusted CA certificate list on the VCS Expressway already contains the public root CA Certificate for the server certificate that the cloud will present. The root CA for the WebEx cloud is DST Root CA X3 with an intermediate CA of Cisco SSCA2.

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.

Step 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 VCS Expressway.

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



```

https://ctg-eft-vcse-1.cisco.com/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN
-----BEGIN CERTIFICATE-----
MIIDISjCCAjKGAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBqkqhkiG9w0BAQUFADA
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDbY4xZAVBgNVBAMTDkRTVCBSb290IENBI
FgzMB4XD
DTAwMDkzMDIxMDIxOVoXDTIxMDkzMDUOMDEuXVowPzEkMCIGA1UEChMhRGlnaXRhbCB
TAWduYXR1cmUgVHJlc3QgQ28uMRcwFQYDVQDEw5EU1QgUm9vdCBDQSBYmzCCASIwDQY
JKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN+v6ZdQcINXtMxiZfaQguzH0yxrMpb7
NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4Orz5Iy2Xu/NmHd2XSKtkyj4z193ewE
nu1lcCJo6m67XMuegWGMoOifooUMMORoOEQOL15CjH9UL2AZd+3UWODYOKIYepLY
YHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRyxXtqzTWMIn
/5WgTe1QlyNau7FqcKh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNADaeQQmxkqt1lX4+U9m5/wA10CAwEAANCM
EAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVRO0BBYEFMSnsa
r7LHH62+FLKHX/xBVghYkQMA0GCSqS5Ib3DQEBBQUAA4IBAQCjGiyFwBcqR7uKGY3Or
+Dxz9Lwmg1SBd491ZRNI+DT69ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faX
bauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYa
LbumR9YbK+r1mM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9S
2ImlJnt1ir/md2cXjbDaJWFbM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJswVijJ
EubSfZGL+T0yJWW06XyxV3bqxYoOb8VZRzI9neWagqNdwYkQsEjgfbKbYK7p2CNTU
Q
-----END CERTIFICATE-----

DST Root CA X3
=====

-----BEGIN CERTIFICATE-----
MIIDISjCCAjKGAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBqkqhkiG9w0BAQUFADA
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDbY4xZAVBgNVBAMTDkRTVCBSb290IENBI
FgzMB4XD
DTAwMDkzMDIxMDIxOVoXDTIxMDkzMDUOMDEuXVowPzEkMCIGA1UEChMhRGlnaXRhbCB
TAWduYXR1cmUgVHJlc3QgQ28uMRcwFQYDVQDEw5EU1QgUm9vdCBDQSBYmzCCASIwDQY
JKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN+v6ZdQcINXtMxiZfaQguzH0yxrMpb7
NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4Orz5Iy2Xu/NmHd2XSKtkyj4z193ewE
nu1lcCJo6m67XMuegWGMoOifooUMMORoOEQOL15CjH9UL2AZd+3UWODYOKIYepLY
YHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRyxXtqzTWMIn
/5WgTe1QlyNau7FqcKh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNADaeQQmxkqt1lX4+U9m5/wA10CAwEAANCM
EAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVRO0BBYEFMSnsa
r7LHH62+FLKHX/xBVghYkQMA0GCSqS5Ib3DQEBBQUAA4IBAQCjGiyFwBcqR7uKGY3Or
+Dxz9Lwmg1SBd491ZRNI+DT69ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faX
bauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYa
LbumR9YbK+r1mM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9S
2ImlJnt1ir/md2cXjbDaJWFbM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJswVijJ
EubSfZGL+T0yJWW06XyxV3bqxYoOb8VZRzI9neWagqNdwYkQsEjgfbKbYK7p2CNTU
Q
-----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 your VCS Expressway is complete.

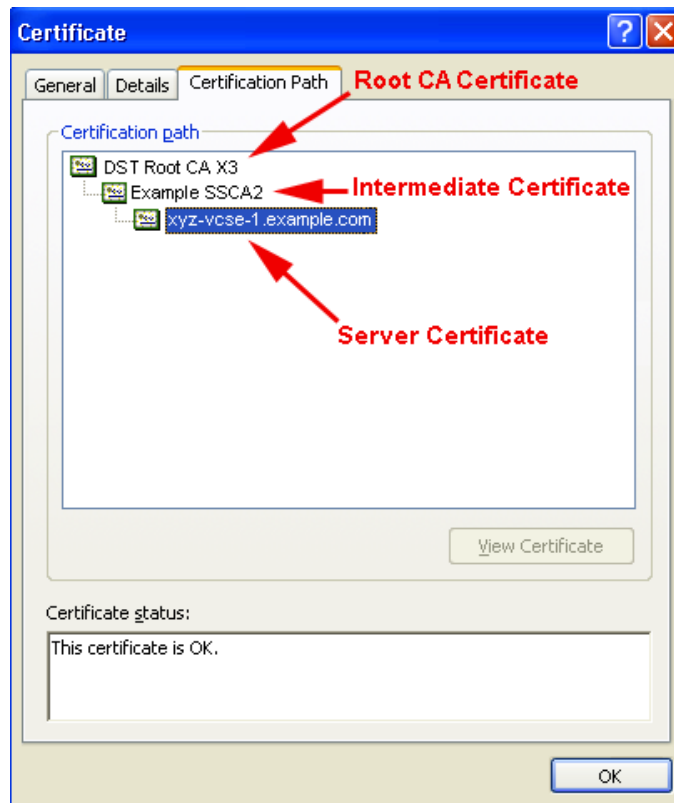
If the server certificate is issued by an intermediate CA or if the certificate for the top-level root CA that issued your server certificate is not part of the trusted CA certificate list, you must add it to the trusted CA certificate list, as detailed in the next section.

Adding the Intermediate CA Certificate to VCS Expressway X8.1

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

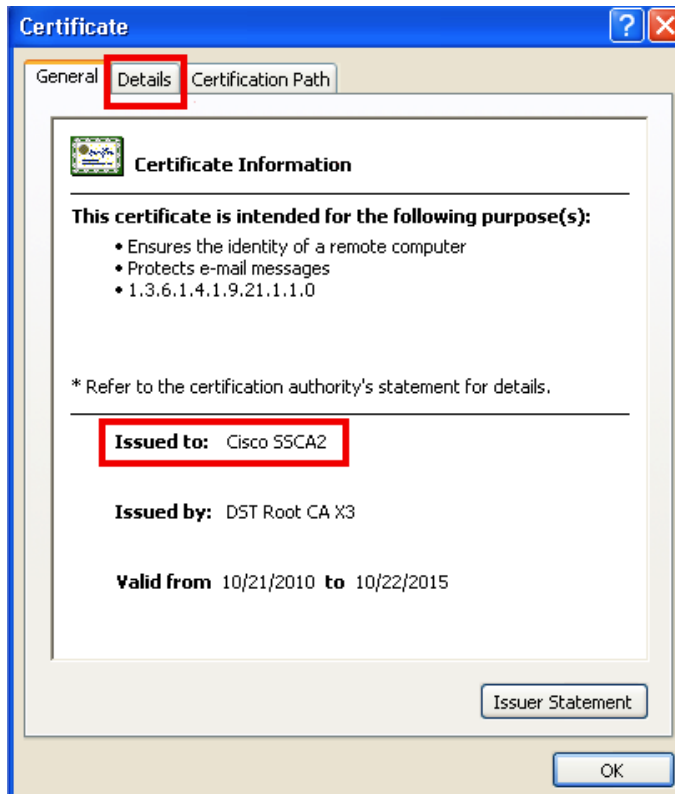
If the server certificate is issued by an intermediate CA, then you'll need to add the intermediate CA certificate to the default trusted CA certificate list.

Figure 5-2 Server Certificate in .CER File Format



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're that you're stacking the correct intermediate CA certificate.

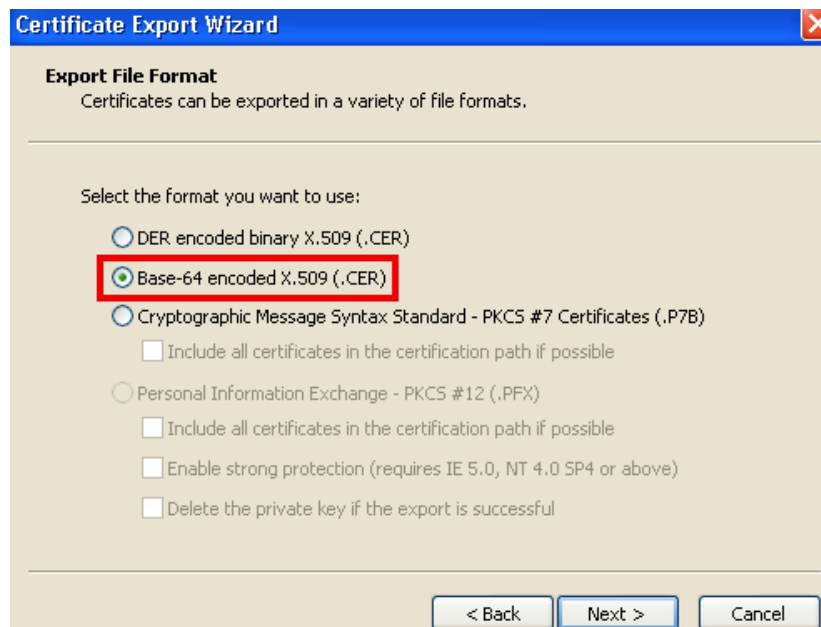
-
- Step 1** Open the server certificate as a .CER file (see [Figure 5-2](#))
 - Step 2** Click the **Certification Path** tab.
 - Step 3** Double-click the **Intermediate Certificate**.
This will open the intermediate CA certificate in a separate certificate viewer.
 - Step 4** Make sure the 'Issued to' field displays the name of the Intermediate CA.
 - Step 5** Click the **Details** tab followed by **Copy to File...**



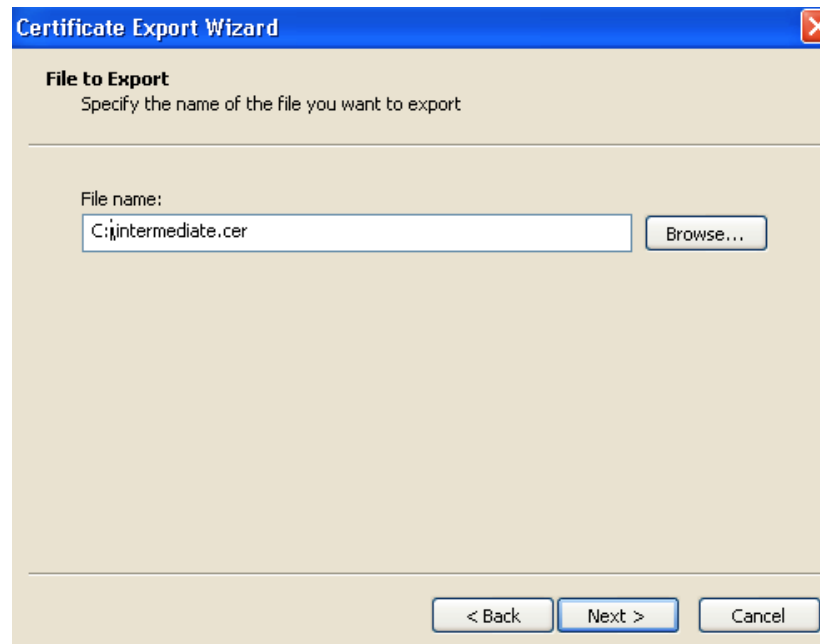
The 'Welcome to the Certificate Export Wizard' appears.

Step 6 Click **Next**.

Step 7 Choose **Base-64 encoded X.509 (.CER)** as the Export File Format and click **Next**.



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



Step 9 Change the extension of your intermediate CA certificate from .cer to .pem.

For example: **intermediate.pem**

Step 10 In VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.

Step 11 Click **Browse**, find your intermediate CA certificate and click **Open**.

Step 12 Click **Append CA certificate**.

Certificate configuration on your 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 the “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 VCS Expressway X8.1

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

- The DST Root CA certificate (the root CA for the WebEx cloud)
- The CA certificate of the CA that issued your server certificate

Adding the DST Root Certificate to VCS Expressway X8.1

Your VCS Expressway must trust the certificate issuer of the server certificate that's passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud, which is DST Root CA.

To add the DST Root certificate to the trusted CA certificate list on VCS Expressway X8.1, do the following:

-
- Step 1** Go to: http://www.identrust.com/doc/SSLTrustIDCAA5_DSTCAX3.p7b
A page with the DST Root certificate contents appears with “-----Begin Certificate-----” at the top.
 - Step 2** Select and copy the entire contents of the page.
 - Step 3** Open a text editor, such as Notepad, on your computer and paste the contents of the DST Root certificate.
 - Step 4** Save the text file with an extension of .PEM. For example: **dst_root_ca.pem**.
 - Step 5** In VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
 - Step 6** Click **Browse**, select the DST Root certificate you saved in step 4 and click **Open**.
 - Step 7** Click **Append CA certificate**.
-

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

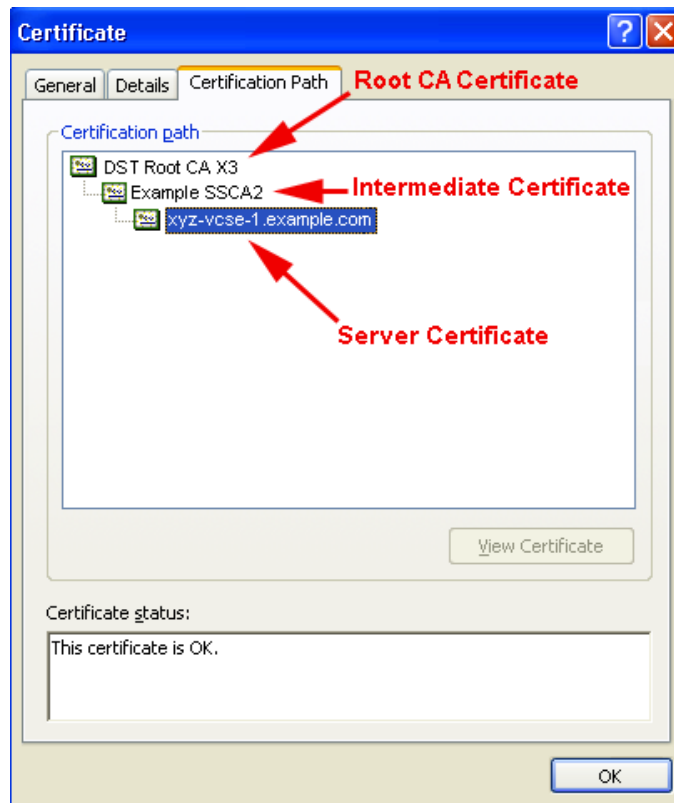
For the WebEx cloud to trust your VCS Expressway's server certificate, you must add the root or intermediate CA certificate for the CA that issued your server certificate.

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 you're that you're stacking the correct intermediate CA certificate.

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

-
- Step 1** Open the server certificate as a .CER file
 - Step 2** Click the **Certification Path** tab. (see [Figure 5-3](#))

Figure 5-3 Server Certificate from Intermediate CA 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 2 certificates (the root and server certificates).

Step 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**.

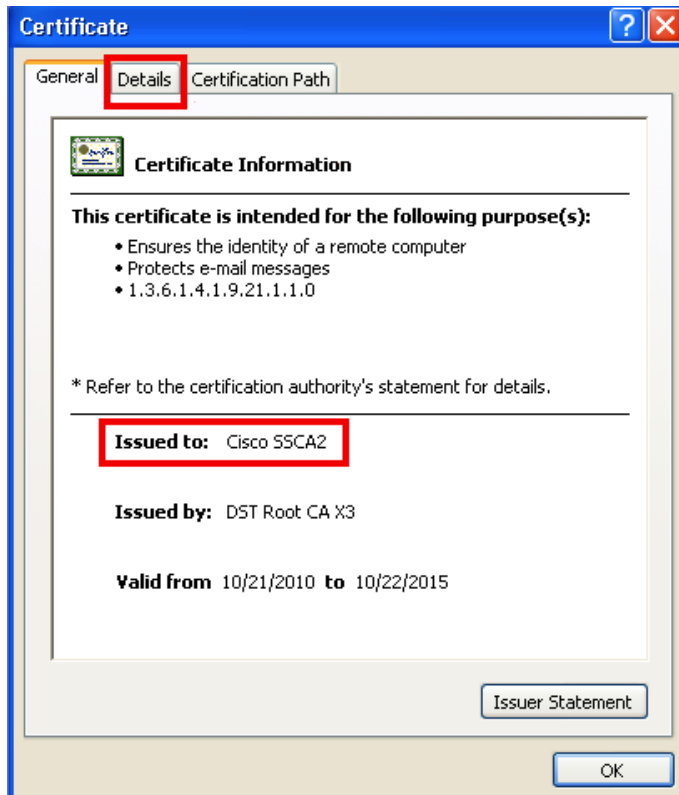
This will open the CA certificate in a separate certificate viewer.

Step 4

Make sure the 'Issued to' field displays the name of the root or intermediate CA.

Step 5

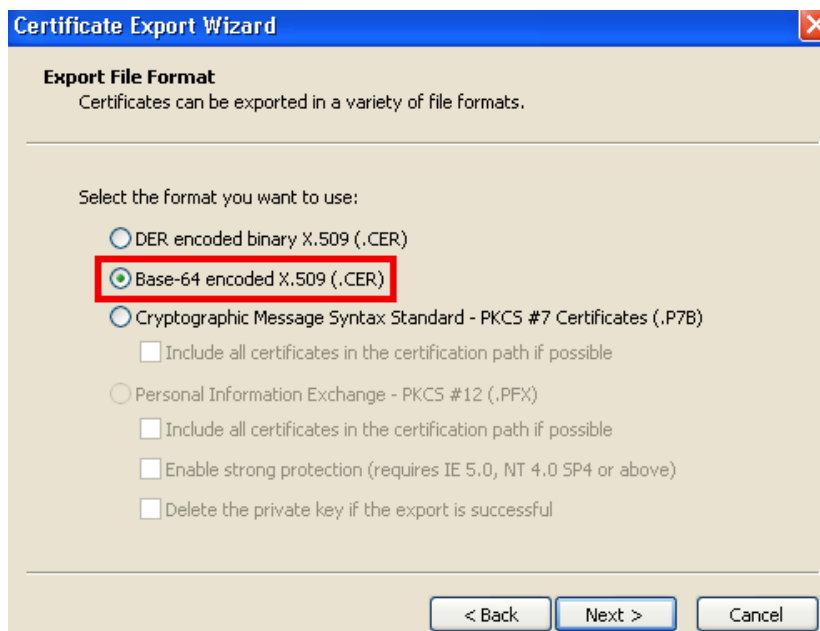
Click the **Details** tab followed by **Copy to File...**



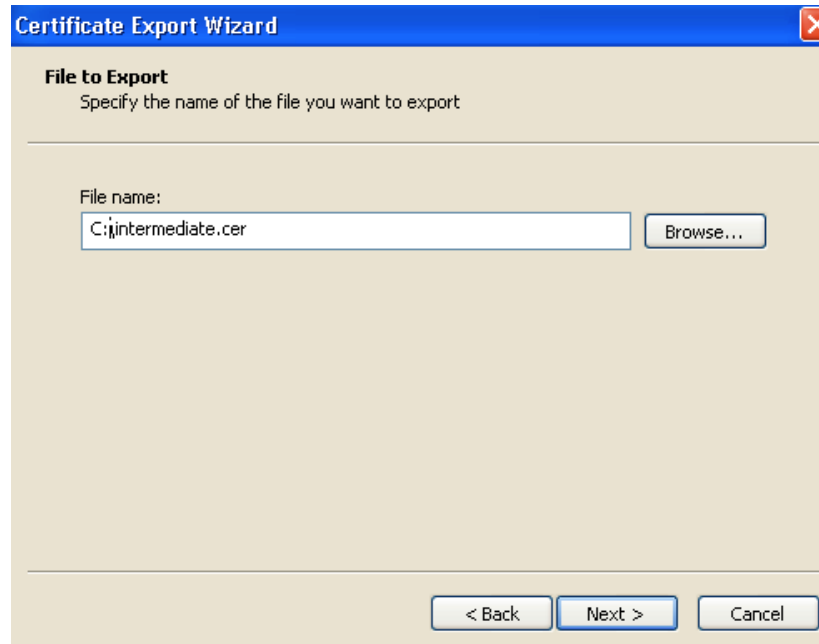
The 'Welcome to the Certificate Export Wizard' appears.

Step 6 Click **Next**.

Step 7 Choose **Base-64 encoded X.509 (.CER)** as the Export File Format and click **Next**.



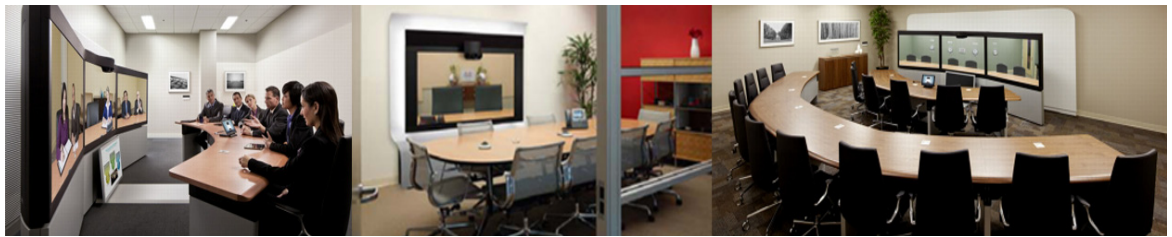
Step 8 Name the file, click **Next**, and **Finish**.



- Step 9** Change the extension of your root or intermediate CA certificate from .cer to .pem.
For example: **root.pem** or **intermediate.pem**
- Step 10** In VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
- Step 11** Click **Browse**, find your root or intermediate CA certificate and click **Open**.
- Step 12** Click **Append CA certificate**.
- Certificate configuration on your 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 the “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



CHAPTER 6

Configuring Cisco TelePresence Management Suite

Revised: October 2015

Contents

This chapter describes how to configure Cisco TelePresence Management Suite (Cisco TMS) for Cisco WebEx Enabled TelePresence meetings. It contains the following sections:

- [Prerequisites, page 6-1](#)
- [Configuring the Cisco WebEx Feature in Cisco TMS, page 6-2](#)
- [Configuring WebEx Users in Cisco TMS, page 6-4](#)
- [Configuring Hybrid Content Mode for MCU in Cisco TMS, page 6-7](#)
- [Configuring Lobby Screen for TelePresence Server in Cisco TMS, page 6-8](#)
- [Configuring Conference Settings in Cisco TMS, page 6-9](#)
- [Configuring Single Sign On in Cisco TMS, page 6-11](#)
- [Supported Configurations for TMS to Schedule on Behalf of the WebEx Host, page 6-18](#)

Prerequisites

- Cisco TMS software release 14.3.1 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
- The WebEx integration option key must be installed on Cisco TMS before configuring the WebEx feature.



Note Multiple WebEx sites are supported.

- 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 Cisco WebEx Enabled TelePresence meetings.
 - For MCU and TelePresence Server, refer to the [Configuring Cisco TelePresence Management Suite, page 6-1](#) for more information.

Configuring the Cisco WebEx Feature in Cisco TMS

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

Step 1 Go to **Administrative Tools > Configuration > WebEx Settings**.

The WebEx Settings page appears. See [Figure 6-1](#).

Figure 6-1 Enabling WebEx in Cisco TMS

The screenshot shows the Cisco TelePresence Management Suite interface. At the top, there is a navigation bar with icons for Portal, Booking, Monitoring, Systems, Phone Books, Reporting, and Adminis. The main heading is 'WebEx Settings' with a breadcrumb 'You are here: > Administr'. Below this is the 'WebEx Configuration' section, which contains three dropdown menus: 'Enable WebEx' (set to 'Yes'), 'Add WebEx To All Conferences' (set to 'Yes'), and 'Get WebEx Username from Active Directory' (set to 'Disabled'). A 'Save' button is located at the bottom of this section. Below the configuration section is the 'WebEx Sites' section, which contains a note: 'When there is more than one site, Cisco TMS will use the default unless a particular site is specified in the user's settings.'

Step 2 Click **Add Site**.

The WebEx Site Configuration page appears. See [Figure 6-2](#).

Figure 6-2 Configuring a WebEx Site

The screenshot shows the Cisco TelePresence Management Suite interface. At the top, there is a navigation bar with icons for Portal, Booking, Monitoring, Systems, Phone Books, Reporting, and Admin. Below this is the 'WebEx Settings' section. The 'WebEx Site Configuration' section contains the following fields:

- Site URL: <https://example.webex.com/example>
- Host Name:
- Site Name:
- WebEx Participant Bandwidth: (dropdown)
- Default Site: (dropdown)
- TSP Audio: (dropdown)
- Use Web Proxy: (dropdown)
- Enable SSO: (dropdown)
- Connection Status: Connection OK

At the bottom of the configuration section, there are two buttons: 'Save' and 'Back'.

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

Step 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*.

Step 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.

Step 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.

Step 7 Set “TSP Audio” to **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.

Step 8 Click **Save**.

Step 9 In the WebEx Configuration section, do the following:

- a. Set “WebEx Enabled” to **Yes**.
- b. Set “Add WebEx To All Conferences” to **Yes**.

Step 10 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, page 6-2](#).

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 a Cisco WebEx Enabled TelePresence User in Cisco TMS, page 6-6](#)
- 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 one 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 Automatic User Lookup from Active Directory, page 6-5](#) and [Configuring Single Sign On in Cisco TMS, page 6-11](#)

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 (e.g. 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:

-
- Step 1** Go to **Administrative Tools > Configuration > Network Settings**.
 - Step 2** In the Active Directory pane, set “Lookup User Information from Active Directory” to **Yes**.
 - Step 3** Enter information in the remaining fields in the Active Directory pane and click **Save**.
- For information about each field, refer to the Cisco TMS Help.
-

To configure ‘Get WebEx Username from Active Directory’, do the following:

-
- Step 1** Go to **Administrative Tools > Configuration > WebEx Settings**.
 - Step 2** 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.
 - Step 3** 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, page 6-11](#).



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 WebEx Enabled TelePresence 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 Automatic User Lookup from Active Directory, page 6-5](#)
- Single Sign On is enabled, as detailed in [Configuring Single Sign On in Cisco TMS, page 6-11](#).
- The user will use the default WebEx site for scheduling WebEx meetings

To configure a Cisco WebEx Enabled TelePresence user in Cisco TMS, do the following:

-
- Step 1** Go to **Administrative Tools > User Administration > Users**
- Step 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**.
- Step 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.
-
- Step 4** For WebEx Username, enter the username for the user’s WebEx account.
- Step 5** For WebEx Password, enter the password for the user’s WebEx account.
- Step 6** For WebEx Site, select the WebEx site to which the user is registered.
-  **Note** If no WebEx site is selected, the WebEx site configured as the default will be used.
-
- Step 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 recommends always enabling port reservations for MCU and TelePresence Server.

Enabling Port Reservations for MCU

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

-
- Step 1** Go to **Systems > Navigator**.
 - Step 2** Select an MCU.
 - Step 3** Click the **Settings** tab.
 - Step 4** Click **Extended Settings**.
 - Step 5** Set “Limit Ports to Number of Scheduled Participants” to **On**.
 - Step 6** Click **Save**.
 - Step 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:

-
- Step 1** Go to **Systems > Navigator**.
 - Step 2** Select a TelePresence Server.
 - Step 3** Click the **Settings** tab.
 - Step 4** Click **Extended Settings**.
 - Step 5** Set “Limit Ports to Number of Scheduled Participants” to **On**.
 - Step 6** Click **Save**.
 - Step 7** Repeat steps 2 through 6 for all other TelePresence Servers.
-

Configuring Hybrid Content Mode for MCU in Cisco TMS

Configuring any MCUs that will be used for Cisco WebEx Enabled TelePresence 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:

-
- Step 1** Go to **Systems > Navigator**.
 - Step 2** Click the MCU name.
 - Step 3** Click the **Settings** tab and then click **Extended settings**.
 - Step 4** Set “Content Mode” to **Hybrid** and click **Save**.
-

Configuring Lobby Screen for TelePresence Server in Cisco TMS

Configuring all TelePresence Servers that will be used for Cisco WebEx Enabled TelePresence 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:

-
- Step 1** Go to **Systems > Navigator**.
 - Step 2** Click the TelePresence Server name.
 - Step 3** Click the **Settings** tab and then click **Extended settings**.
 - Step 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 TMS. [Table 6-1](#) 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 WebEx Enabled TelePresence meetings as described in the previous section.

Table 6-1 *Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled*

TelePresence Server Lobby Screen Setting	WebEx Enabled TelePresence 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)
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 WebEx Enabled TelePresence meetings.

Default Setup and Teardown Buffers

Cisco recommends configuring the default setup and teardown buffers so that the TelePresence portion of the meeting starts and ends at the scheduled time.



Note

Users scheduling a meeting using TMS, can change the setup and teardown buffers for each individual meeting if they want to.

To configure default setup and teardown buffers Cisco TMS, do the following:

-
- Step 1** Go to **Administrative Tools > Configuration > Conference Settings**.
- Step 2** In the Conference Create section, make the following settings:
- For Default Setup Buffer, select **0**.
 - For Default Tear Down Buffer, select **0**.
- Step 3** Click **Save**.
-

Default Picture Mode

Cisco recommends configuring Default Picture Mode to Continuous Presence. This allows multiple participants to be seen on screen at the same time for meetings that use MCU. TelePresence Server is always set to display multiple participants (called ActivePresence on the TelePresence Server).


To configure Default Picture Mode in Cisco TMS, do the following:

-
- Step 1** Go to **Administrative Tools > Configuration > Conference Settings**.
- Step 2** In the Conference Create Options section, set the following option:
- For Default Picture Mode, select **Continuous Presence**.
- Step 3** Click **Save**.
-

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:

-
- Step 1** Go to **Administrative Tools > Configuration > Conference Settings**.
- Step 2** In the Conference Connection/Ending Options section, set the following options:
- 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.
-
- 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



Note 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.

- (Optional) You can configure the length, timing and content of the in-video warnings, by setting the following options:
 - Message Timeout (in seconds): The number of seconds that a warning message will be displayed. Default setting: 10 seconds.
 - 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).



Note For TelePresence MPS bridges, only 10, 5 and 1 can be entered here and will be displayed as a number icon on the screen. All other systems can be configured with any number intervals, and will show the Meeting End notification followed by the text string entered in Contact Information to Extend Meetings.

- 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.
- 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.

Step 3 Click **Save**.

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, page 6-2](#) for details.

2. Generate a certificate to secure the connection between Cisco TMS and the WebEx site.

See [Generating a Certificate for WebEx, page 6-13](#) for details.

3. Enable Partner Delegated Authentication on the WebEx site.

See [Enabling Partner Delegated Authentication on the WebEx site, page 6-16](#) for details.

4. Enable SSO in Cisco TMS.

See [Enabling SSO in Cisco TMS, page 6-17](#) 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:

-
- Step 1** Using the Windows Certificate Manager Snap-in, export the existing key/certificate pair as a PKCS#12 file.
 - Step 2** Using the Windows Certificate Manager Snap-in, export the existing certificate as a Base64 PEM encoded .CER file.
 - Step 3** Make sure the certificate is in .cer or .crt format and provide this file to the WebEx Cloud Services team.
 - Step 4** Use the PKCS#12 file you created in step 2, to upload to TMS in [Enabling SSO in Cisco TMS, page 6-17](#)

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:

-
- Step 1** Use Windows Certificate Manager Snap-in to export your existing certificate in a Base64 PEM file.
 - Step 2** Change the file extension to .cer or .crt and provide this file to the WebEx Cloud Services team.
 - Step 3** Create a PKCS#12 key/certificate pair by using the command in step 10 of [Using OpenSSL to Generate a Certificate, page 6-14](#).

- Step 4** Use this PKCS#12 file to upload to TMS in [Enabling SSO in Cisco TMS, page 6-17](#).
-

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 [Using OpenSSL to Generate a Certificate, page 6-14](#).

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:

- Step 1** Create a new key/certificate pair to use for the WebEx SSO configuration using OpenSSL, following the steps in [Using OpenSSL to Generate a Certificate, page 6-14](#).
- Step 2** Create a Base64 PEM encoded version of the signed certificate using step 8 [Using OpenSSL to Generate a Certificate, page 6-14](#)
- Step 3** Change the file extension of this signed certificate to .cer or .crt and provide this version of the certificate to the WebEx Cloud Services team.
- Step 4** Create a PKCS#12 key/cert pair by using the command in step 10 of [Using OpenSSL to Generate a Certificate, page 6-14](#).
- Step 5** Use this PKCS#12 file to upload to TMS in [Enabling SSO in Cisco TMS, page 6-17](#).
-

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:

- Step 1** Follow the steps in [Using OpenSSL to Generate a Certificate, page 6-14](#).
- Step 2** In step 6, follow the procedure to create a self-signed certificate signing request.
- Step 3** Follow steps 7 through 9 and provide the base64 PEM file of self-signed certificate to the WebEx Cloud Services team.
- Step 4** Follow step 10 to create a PKCS#12 PFX file
- Step 5** Upload to TMS in [Enabling SSO in Cisco TMS, page 6-17](#).
-

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. Change the file extension of the signed certificate to .cer or .crt and provide it to the WebEx cloud services 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

To use OpenSSL to generate a certificate, do the following:

-
- Step 1** In Windows, open a command prompt.
- Step 2** Navigate to the openssl\bin installation directory.
- Step 3** Generate a private key using following command:
- ```
openssl genrsa -out tms-privatekey.pem 2048
```
- Step 4** 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
```
- Step 5** 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
- Step 6** 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.
- Step 7** 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**.

- Step 8** 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.

- Step 9** Change the file extension of this signed certificate to .cer or .crt and provide it to the WebEx Cloud Services team.

- Step 10** 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 [Enabling Partner Delegated Authentication on the WebEx site](#) 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 [Enabling SSO in Cisco TMS, page 6-17](#) 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 [Generating a Certificate for WebEx, page 6-13](#).
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”.

To enable partner delegated authentication on your WebEx site, do the following:

- Step 1** Log into your WebEx administrative site and go to **Manage Site > Partner Authentication**.

The Partner Delegated Authentication page appears.

Figure 6-3 Partner Delegated Authentication on the WebEx Administrative Site

The screenshot shows the WebEx Site Administration interface. The top navigation bar includes the WebEx logo and the title "Site Administration". A sidebar on the left contains navigation links for Home, Manage Site (Site Settings, Tracking Codes, Company Addresses, Email Templates, Meetings in Progress, SSO Configuration, Partner Authentication), Manage Users (Edit wbxadmin, Add User, Edit User List, Import/Export Users, Edit Privileges, Send Email to All), Session Types (Add Custom Type, Session Type List), Assistance (Help), and Log out. The main content area is titled "Partner Delegated Authentication" and contains a section for "Partner SAML Authentication Access". This section has a table with columns for Host, Site Admin, and Partner Certificate. The Host and Site Admin columns have checked checkboxes. The Partner Certificate column shows "examplesso.webex.com" and a "View Details" link. Below the table are "Update" and "Cancel" buttons. At the bottom, there is a "POWERED BY Cisco WebEx Technology" logo and a copyright notice: "© 2012 Cisco and/or its affiliates. All rights reserved. www.webex.com Privacy | Terms of Service".

- Step 2** 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 [Enabling Partner Delegated Authentication on the WebEx site, page 6-16](#).

To enable SSO in Cisco TMS, do the following:

- Step 1** Log into Cisco TMS, and go to **Administrative Tools > Configuration > WebEx Settings**.
- Step 2** In the WebEx Sites pane, click the site name of the WebEx site on which you want to enable SSO. The WebEx Site Configuration pane appears.
- Step 3** For Enable SSO, select **Yes**. The SSO Configuration pane appears.

- Step 4** Click **Browse** and upload the PKS #12 private key certificate (.PFX) you generated in [Generating a Certificate for WebEx, page 6-13](#).
- Step 5** Complete the rest of the SSO configuration fields using the password and other information that you selected when generating the certificate.
- Step 6** Click **Save**.

Figure 6-4 WebEx Settings SSO Configuration in Cisco TMS

WebEx Settings You are here: Administrative Tools > Configuration > WebEx

WebEx Site Configuration

Site URL:

Host Name:

Site Name:

WebEx Participant Bandwidth:

Default Site:

TSP Audio:

Use Web Proxy:

Enable SSO:

Connection Status: Connection OK

SSO Configuration

Certificate:

Upload Certificate:

Certificate Password:

Partner Name:

Partner Issuer (IdP ID):

SAML Issuer (SP ID):

AuthnContextClassRef:

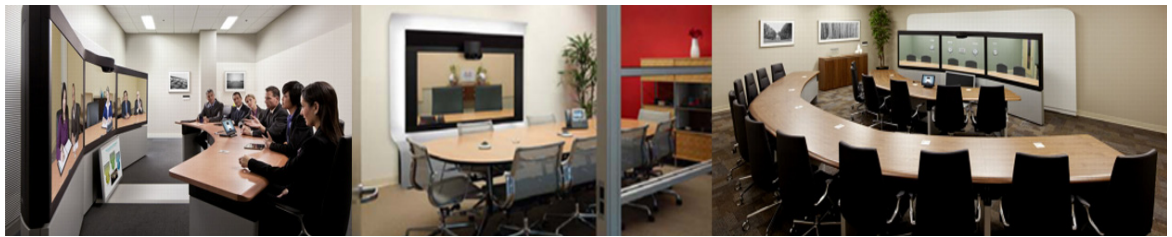
Supported Configurations for TMS to Schedule on Behalf of the WebEx Host

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 WebEx Enabled TelePresence meetings.

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

1. 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.
2. 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.
3. 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 TMS. TMS is trusted to schedule for that user.



CHAPTER 7

Configuring Cisco TelePresence Management Suite Extension for Microsoft Exchange

Revised: May 2013

Contents

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

- [Prerequisites, page 7-1](#)
- [Deployment Best Practices, page 7-2](#)
- [Scheduling Options with TMSXE, page 7-2](#)
- [Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook, page 7-2](#)
- [Configuring Cisco TMSXE for the WebEx Scheduling Mailbox, page 7-6](#)

Prerequisites

- Cisco TMSXE software release 3.1 or later is required.
- Cisco TMS software release 14.2 or later is required.
- Endpoints that are available as mailboxes for booking in a Cisco WebEx Enabled TelePresence 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 3.1.2](#)

Scheduling Options with TMSXE

With TMSXE, there are two options for scheduling:

- 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:

-
- Step 1** On the Cisco TMSXE server, go to the Control Panel.
- Step 2** Right-click **Cisco TelePresence Management Suite Extension for Microsoft Exchange** and select **Change**.
- This starts the installer and allows you to change your installation.
- Step 3** 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](#).



Warning

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):

-
- Step 1** Open the Server Manager console (Start > All Programs > Administrative Tools > Server Manager).
- Step 2** In the Role View, select IIS Manager (Server Manager > Roles > Web Server > IIS Manager).
- Step 3** Double-click **Server Certificates**.
- Step 4** In the Actions pane on the right, click **Create Certificate Request**.
- Step 5** (Important) In the “Common Name:” field, enter the Fully Qualified Domain Name (FQDN) of the DNS name which users will type into the address bar in their browser to reach your website (site.cisco.com NOT site). If you have a different physical hostname than what users will type into their browsers to get to your site, make sure to put in the name users will use.
- Step 6** In the “Organization” field, type your organization name.
- Step 7** In the “Organizational Unit” field, type the name of your organization and click **Next**.
- Step 8** In the “City/locality” field, type the city where the server resides and click **Next**.
- Step 9** In the “State/province” field, type the state where the server resides.

- Step 10** In the “Country/Region” field, select US (United States) and click **Next**.
- Step 11** Leave the CSP at the default value.
- Step 12** For the “Bit Length”, select 2048.
- Step 13** Enter (or Browse to) a filename to save the certificate request (CSR), click **Finish**.
- Step 14** Copy and paste the entire contents of the CSR file you just saved.
The default save location is C:\.
- Step 15** Provide the CSR file to your CA and wait for them to send a signed certificate back to you.

Installing the Public Root Certificate in IIS7 (Windows Server 2008):

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

Installing the Intermediate CA certificate (if applicable):

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

Installing your SSL server certificate:

- Step 1** In the IIS Manager console, go to the **Server Certificates** action pane, and click **Complete Certificate Request**. The Complete Certificate Request Wizard appears.
- Step 2** Browse to the location where you saved your SSL server certificate, select it, then click **Open**.
- Step 3** Enter a friendly name for your certificate (use the certificate's hostname if you're unsure). Then click **OK**.
At this point SSL is available for TMSXE. You will still need to configure the TMSXE or individual directories to use SSL. Select your IIS Site.
- Step 4** In the action pane on the right, under Edit Site, click **Bindings**.
- Step 5** Click the **Add** button.
- Step 6** In the Type menu, select **https**.

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

Setting Up Communication Between Your WebEx Site and TMSXE

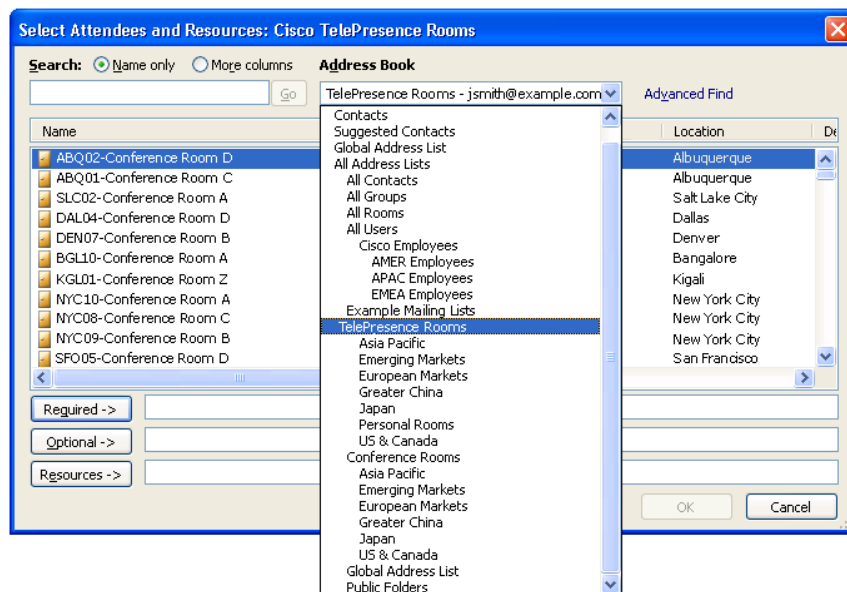
Follow the steps described in [Cisco TelePresence Cisco WebEx Integration Options, page 10-1](#)

Configuring the Location Displayed for TelePresence Rooms in Outlook

When selecting telepresence rooms while scheduling a WebEx Enabled TelePresence meeting in Outlook, the location of the room is displayed in the both the Select Attendees and Resources Address Book window (Figure 7-1), which is a standard part of Outlook, and the Select Telepresence Rooms window (Figure 7-2), which is displayed when using the WebEx and TelePresence Integration to Outlook.

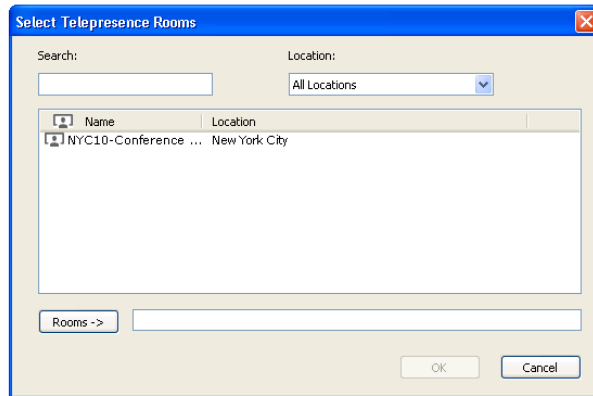
- To display the Select Attendees and Resources Address Book window, click the **To...** button in the Meeting window.

Figure 7-1 Select Attendees and Resources - Address Book



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

Figure 7-2 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 [Figure 7-1](#).

The structure and hierarchy displayed in the drop-down menu in the Exchange Address Book ([Figure 7-1](#)) 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: [Installing the WebEx and TelePresence Integration to Outlook, page 10-6 of Chapter 10, “Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account”](#).

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:

-
- Step 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 \(Exchange 2007 Help\)](#).

Step 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 \(Exchange 2007 Help\)](#).

Step 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:

Step 1 Log in to the server on which TMSXE is installed.

Step 2 From the Windows task bar, select **Start > All Programs > Cisco > TMSXE Configuration**.

Step 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.

Step 4 Click the **Exchange Web Services** tab.

Step 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.

Step 6 Click **Save**.

TMSXE validates the email address you provided and a message appears indicating your settings have been saved.

Step 7 Click **Exit**.

Additional Recommendations

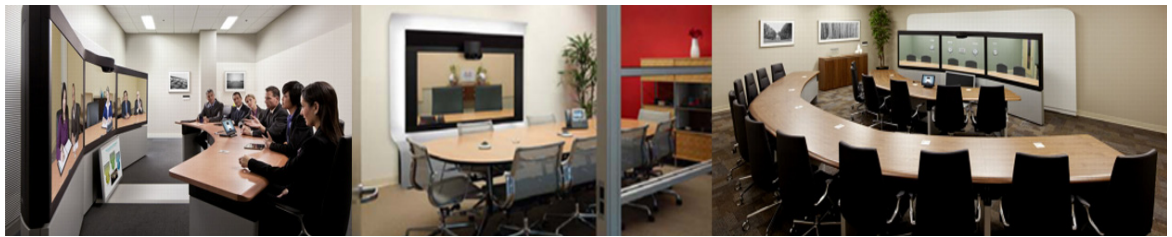
Cisco also recommends using the following configurations for WebEx Scheduling Mailbox:

- Using Exchange Management Console Mail Flow Settings or Powershell, stricthen 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.



CHAPTER 8

Configuring Cisco TelePresence Management Suite Provisioning Extension

Revised: November 2013

Contents

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

- [Prerequisites, page 8-1](#)
- [Introduction, page 8-2](#)
- [User Access to Cisco TMSPE, page 8-2](#)
- [How Smart Scheduler Works, page 8-3](#)
- [Limitations, page 8-4](#)

Prerequisites

- Cisco TMS software release 14.2 or later must be installed.
- Cisco TMSPE software release 1.1 or later must be installed and enabled in TMS.
 - For details, refer to the [Cisco TelePresence Management Suite Provisioning Extension Deployment Guide](#).
- WebEx must be configured on 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 TMS, refer to [Configuring Cisco TelePresence Management Suite](#).

- Smart Scheduler requires one of the following browsers:
 - Internet Explorer - version 9 or later
 - Mozilla Firefox - version 10 or later
 - Safari - version 6 or later
 - Chrome - version 24 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 8-1 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.

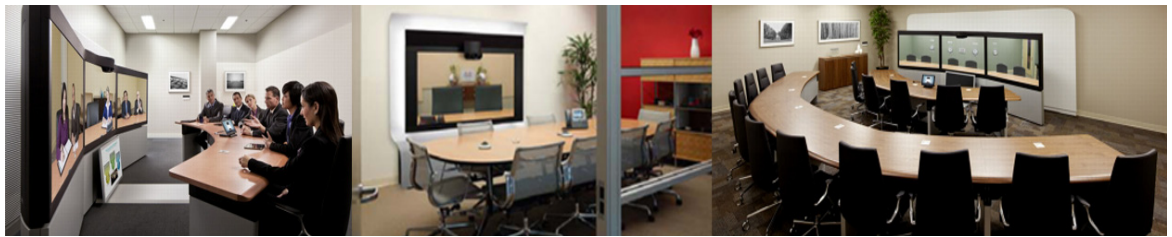
If the Cisco TMSPE user does not already exist in Cisco TMS, it will be created at the same time as the booking.

4. 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 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.
- Smart Scheduler is not compatible with the use of setup and teardown buffers in Cisco TMS scheduling. This is a limitation of the Cisco TelePresence Management Suite Extension Booking API.



CHAPTER 9

Configuring Audio

Revised: November 2013

Contents

This chapter describes how to configure audio for Cisco WebEx Enabled TelePresence.

The following sections describe the audio deployment scenarios:

- [Configuring SIP Audio for Cisco WebEx Enabled TelePresence, page 9-2](#)
- [Configuring PSTN Audio for Cisco WebEx Enabled TelePresence, page 9-3](#)
- [Configuring TSP Audio for Cisco WebEx Enabled TelePresence, page 9-7](#)

Prerequisites

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

- VCS Control/Expressway must be configured.
For details, refer to: [Chapter 4, “Configuring Cisco TelePresence Video Communication Server Control and Expressway”](#).
- When using Unified CM, make sure:
 - SIP trunk is configured between Unified CM and VCS Control.
For details, see [Configuring a SIP Trunk Between Unified CM and VCS Control, page 4-5](#)
 - Your regions are configured for g.711.
- If configuring PSTN audio, Gateway must be registered to VCS or 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 Conductor is not supported at this time.

Configuring SIP Audio for Cisco WebEx Enabled TelePresence

The following section describes the steps required for configuring SIP audio for Cisco WebEx Enabled TelePresence.

This section describes the following:

- [Configuring the WebEx Site in Cisco TMS to Use SIP Audio](#)
- [Enabling Hybrid Audio on the WebEx Site, page 9-3](#)



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:

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

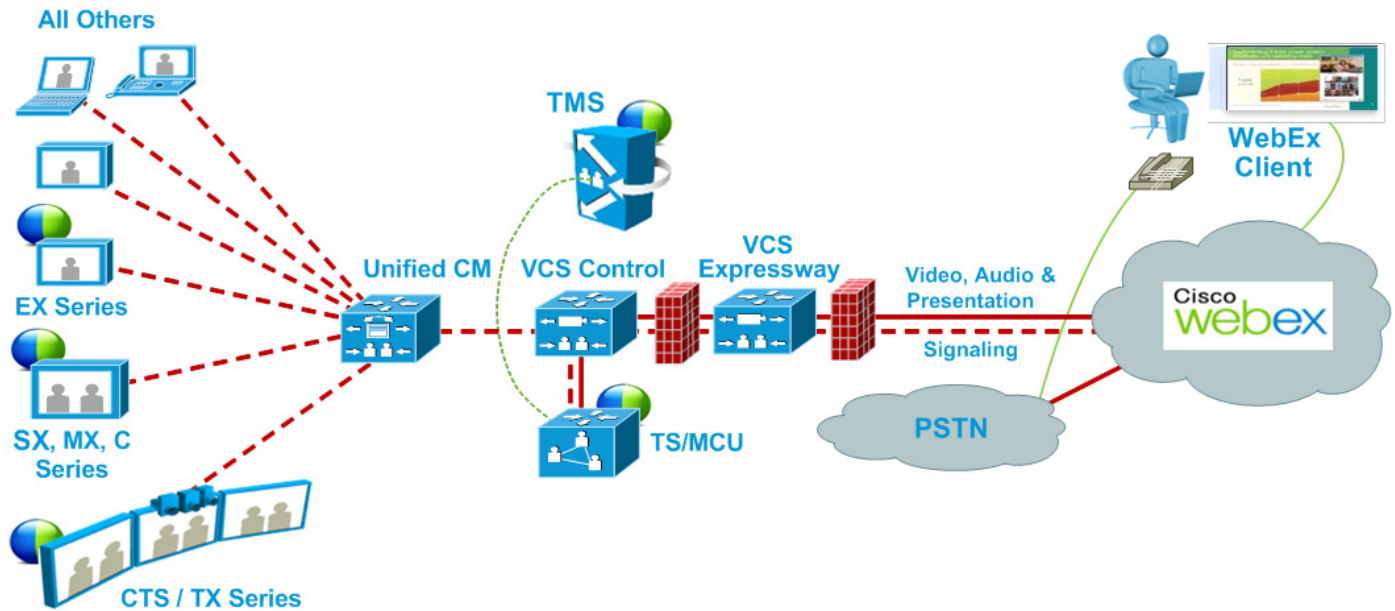
Enabling Hybrid Audio on the WebEx Site

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://support.webex.com/MyAccountWeb/GPLWebForm.do>

Figure 9-1 SIP Audio Deployment with Endpoints Registered to Unified CM



Configuring PSTN Audio for Cisco WebEx Enabled TelePresence

The following section describes the steps required for configuring PSTN audio for Cisco WebEx Enabled TelePresence.

This section describes the following:

- [Configuring the WebEx Site in Cisco TMS to Use PSTN Audio](#)
- [Enabling Hybrid Mode on the WebEx Site, page 9-4](#)
- [Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx, page 9-4](#)



Note

Cisco WebEx Enabled TelePresence 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:

-
- Step 1** Log into Cisco TMS.
- Step 2** Go to **Administrative Tools > Configuration > WebEx Settings**.
The WebEx Settings page appears.
- Step 3** Click the name of the WebEx site you want to configure.
The WebEx Site Configuration page appears.
- Step 4** If a new site, enter the Site Name, Host Name and other required fields.
- Step 5** For TSP Audio, select **Yes**.
- Step 6** 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 VCS, page 9-4](#)
- [Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Unified CM, page 9-6](#)

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

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

-
- Step 1** 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).

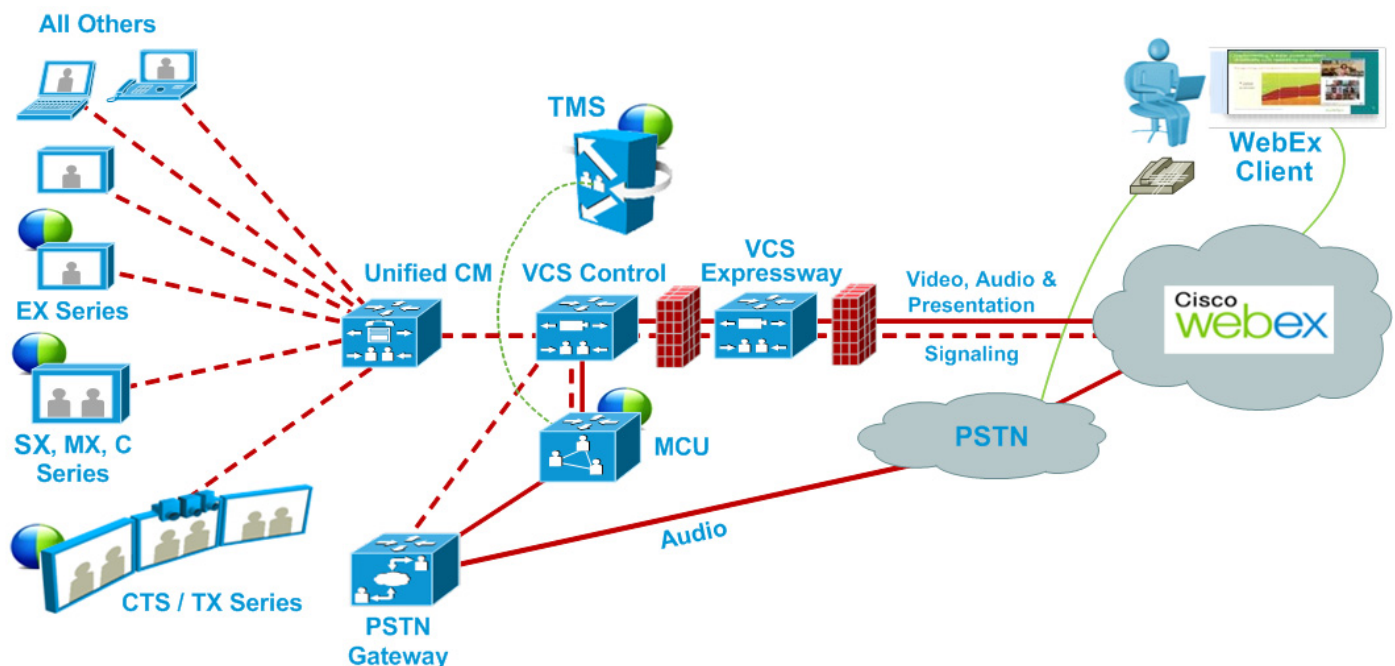
This example transforms **+14085551212@example.webex.com** to **9#14085551212@example.webex.com** using the Regexp pattern type:

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

For more information about configuring traversal zones, search rules and transforms in VCS, 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

Figure 9-2 PSTN Audio Deployment with Gateway Registered to VCS and Endpoints Registered to Unified CM



Configuring 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 VCS Control.



Note

This step is required only for ISDN gateways.

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

- Step 1** Log in to VCS Control.
- Step 2** Go to **VCS Configuration > Protocols > Interworking**.
- Step 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:

- Step 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.
- Step 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.

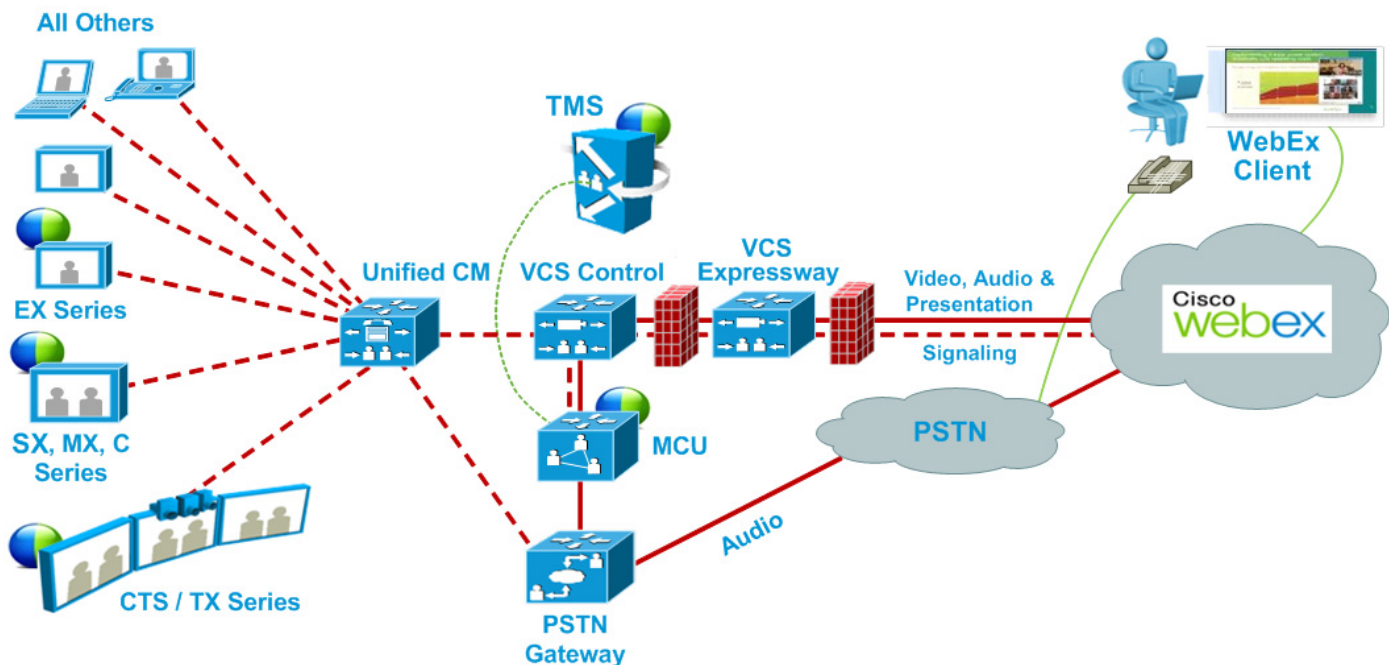
For more information about configuring search rules on VCS, refer to the “Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide” at:

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

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 9-3 PSTN Audio Deployment with Gateway and Endpoints Registered to Unified CM



Configuring 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 VCS Control.



Note This step is required only for ISDN gateways.

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

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



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

Verifying the Outbound Dialing Configuration for VCS and MCU/TelePresence Server

To verify that outbound dialing is properly configured, do the following:

- Step 1** Immediately after call is placed, on the VCS Control navigate to Status -> Search history
- Step 2** Determine if the call appears in the search history:
 - a. If the call does not appear here, then the MCU never dialed out. Enable SIP/H323 logs on the MCU. Replace the call, stop SIP/H323 logging, and download the logs.
 - b. If the call does appear here, click on view for the call under the actions header. This will display the detailed search history.
- Step 3** Within the detailed search history, in the first subsearch it should show transforms. The value listed below here is the exact URI that you are calling after the transforms take effect. Later on, you should do a subsearch that points to the Zone for the external dial-out (usually Unified CM). The alias listed here is exactly as you are presenting the call to the other side. Make sure that the other side is expecting the call in this formation (ie: no “+” characters or anything the other side might not support).
- Step 4** If the search on the other side shows “Found: False” look at the Reason. If the Reason is Not Found, then the other side is returning a 404. In this case, make sure that the following are taking place:
 - a. The VCS is passing the URI EXACTLY as the other side is expecting
 - b. The other side is configured to allow the call.

Configuring TSP Audio for Cisco WebEx Enabled TelePresence

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

**Note**

The TSP provider must support the Call-in User Merge. 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.

There are four required parts to TSP audio configuration:

- [Configuring MACC Domain Index and Open TSP Meeting Room Webex Settings](#)
- [Configuring the TSP Dial String](#)
- [Configuring How the Conference is Opened](#)
- [Configuring TSP Audio for the Meeting Organizer](#)

For more information, refer to:

- [Overview of TSP Audio Configuration and Meetings](#)

**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, please review the section: [Configuring PSTN Calls to Pass through a PSTN Gateway Registered to VCS, page 9-4](#).

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

During a meeting that uses TSP audio, TelePresence equipment dials into the TSP partner's bridge and navigates the menu hierarchy to connect to the conference. The audio (IVR) prompts for each TSP provider are different. As a result, a DTMF dial string must be created.

DTMF Dial String

A static DTMF dial string must be created and tested by your TSP audio provider and then provided to Cisco WebEx cloud services. WebEx cloud services then configures the dial string parameters in the WebEx cloud for your WebEx site. The following is an example sequence of what needs to be provided:

1. MCU/TelePresence Server dials 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)
- For more information, contact Cisco WebEx cloud services.

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 9-4 WebEx Host Account / TSP Audio Account

Configuring How the Conference is Opened

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

Until the host dials in (by entering the host key) participants are in a waiting room. If the host is late or never dials in and unlocks via WebEx, the meeting will never get unlocked.

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:** Configure the DTMF dial string for the MCU/TelePresence Server to enter the meeting as the host and unlock the meeting.
 - WebEx cloud services works with the TSP partner to create the proper DTMF dial string.
 - If the WebEx host has already entered meeting, the DTMF dial string of the MCU/TelePresence Server will be heard by meeting participants.



Note

A DTMF dial string is required, whether or not you are configuring the dial string for the MCU/TelePresence Server to enter the meeting as host. 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. Contact your TSP provider to determine if they support this API command.

How TSP Integration Methods Affect Call Scenarios

The following table describes common scenarios and the results depending on which method is used to open the conference.

Table 9-1 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 audio.
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.
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: <ul style="list-style-type: none"> a. all attendees have left the conference or b. TSP API sends W2A_CloseConference

Scenario	Expected Result	If method 1 is used	If method 2 is used
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	MCU should fail to join	MCU/TelePresence Server should fail to join

Configuring TSP Audio for the Meeting Organizer

Each meeting organizer who needs to schedule WebEx Enabled TelePresence 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.

Prerequisites

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

Configuring TSP Audio

To configure TSP audio, do the following:


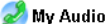
-
- Step 1** Open a browser and go to your WebEx site. (Example: <http://example.webex.com>)
 - Step 2** In the upper part of the page, click **My WebEx**. 
 - Step 3** Enter the **Username** and **Password** for your WebEx account and click **Log In**.
 - Step 4** In the left-hand side of the page, click **My Audio**. 
 - Step 5** In the Teleconferencing Service Accounts section, click **Add account**.
 - Step 6** In the Add Teleconferencing Account window, enter the appropriate phone numbers and access codes for the host and attendees, as provided by the TSP audio service provider.

Figure 9-5 Add Teleconferencing Account window

Add Teleconferencing Account

Call-in toll-free number: Toll-free

Call-in number: Toll-free

Host access code:

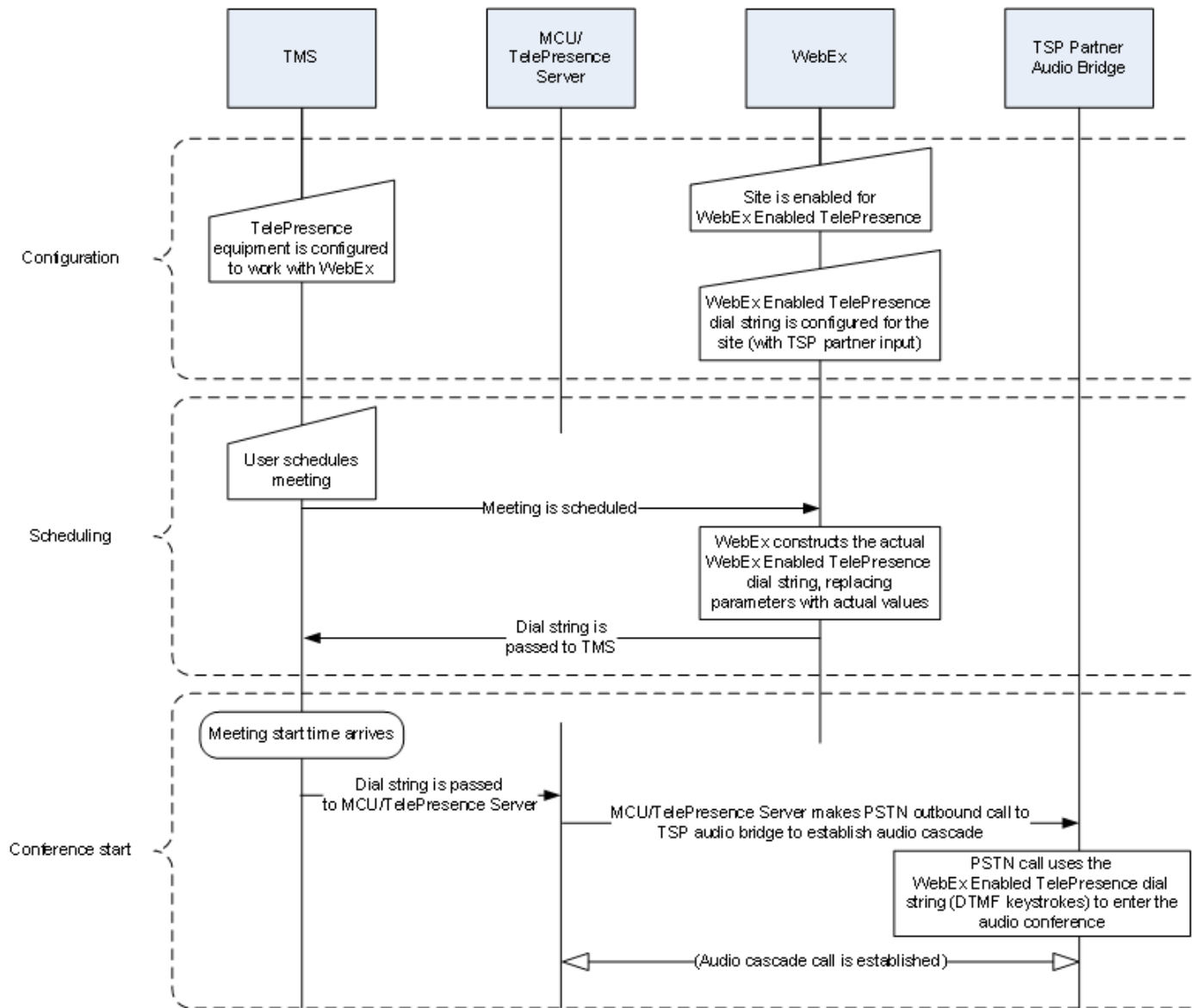
Attendee access code:

Step 7 Click **OK**.

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 9-6 TSP Audio Configuration, Scheduling and Meeting Start Flow



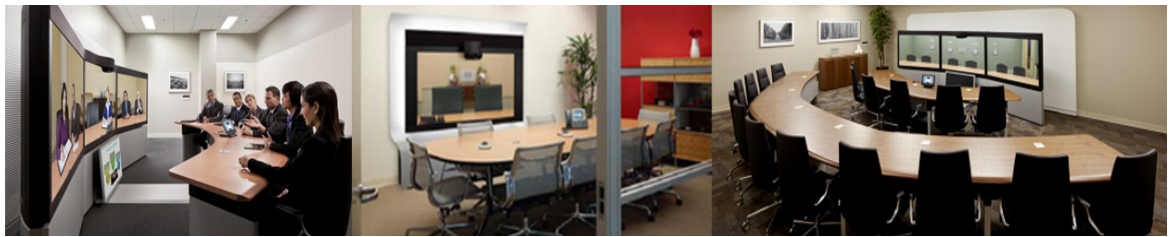
How a TSP Meeting Works

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.



CHAPTER 10

Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account

Revised: November 2013

Contents

This chapter describes how to configure your WebEx site for Cisco WebEx Enabled TelePresence. It contains the following sections:

- [Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account](#), page 10-1
- [Assigning the Meeting Center TelePresence Session Type](#), page 10-3
- [Network-Based Recording of WebEx Enabled TelePresence Meetings](#), page 10-6
- [Installing the WebEx and TelePresence Integration to Outlook](#), page 10-6
- [Setting the Time Zone and Language Preferences for a User's WebEx Account](#), page 10-8
- [Configuring TSP Audio for a User's WebEx Account](#), page 10-9

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:

- [Cisco TelePresence Cisco WebEx Integration Options](#), page 10-1
- [Assigning the Meeting Center TelePresence Session Type](#), page 10-3

Cisco TelePresence Cisco WebEx Integration Options

To integrate Cisco TelePresence to Cisco WebEx:

- Step 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>
- Step 2** On the left navigation bar under **Manage Site**, choose **Site Settings**. The Site Settings screen appears.
- Step 3** Scroll down to OneTouch TelePresence Options, as shown in [Figure 10-1](#).

Figure 10-1 Configuring Cisco WebEx Connection Settings

The screenshot shows the Cisco WebEx Site Administration interface. The top navigation bar includes 'Home', 'Manage Site', 'Manage Users', 'Session Types', 'Assistance', and 'Log out'. The 'Manage Site' section is expanded, showing 'Site Settings' as the selected option. The main content area is titled 'Site Settings for: Common' and includes a dropdown menu for selecting a service. Below this, the 'OneTouch TelePresence Options' section is visible. It contains several checkboxes and a text input field. The 'Allow Cisco WebEx OneTouch meetings (MC only)' checkbox is checked. The 'Cisco TMS booking service URL' field contains 'https://ctg-alpha-scheduler1.cisco.com'. The 'List TelePresence meetings on calendar' checkbox is checked. The 'Send invitation email to meeting host' checkbox is unchecked. The 'Display toll-free number to participants' checkbox is checked. The 'Enable TelePresence bandwidth control' checkbox is checked. The 'Display TelePresence welcome screen' checkbox is unchecked. A red box highlights the 'WebEx VoIP and video connection' section, which has radio buttons for 'Automatically encrypted UDP/TCP SSL' (selected) and 'TCP SSL', and a checkbox for 'Disable Hybrid VoIP' (unchecked).

- Step 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.
- Step 5** If you are deploying the Cisco WebEx Enabled TelePresence 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. For more information about configuring TMSXE, see [Chapter 6, “Configuring Cisco TelePresence Management Suite.”](#)
- Step 6** Click to select **List Cisco TelePresence meetings on calendar** so that scheduled meetings appear on the Cisco WebEx calendar.
- Step 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.
- Step 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.
- Step 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.
- Step 10** In the WebEx VOIP and video connection field, click one of the following:
- **Automatically encrypted UDP/TCP SSL—(Recommended)** Allows the TelePresence Server or MCU to connect over UDP with the Cisco TelePresence Gateway. If the UDP connection is not allowed, TelePresence Server or MCU will fall back to TCP.

- **TCP SSL**—Connects over TCP over a SSL connection.

This selects the connection method between the Cisco WebEx client and the multimedia server (VOIP and video).

Step 11 (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 WebEx-enabled TelePresence meetings.

Step 12 Scroll to the bottom of the page and click **Save** to save your settings.

Step 13 Proceed to [Assigning the Meeting Center TelePresence Session Type](#) 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, page 10-3](#)
- [Adding the Cisco TelePresence Session Type in the Edit User Screen, page 10-5](#)

Support for Custom Session Types

Custom session types can now 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 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

Step 1 In the left navigation bar under **Manage Users**, choose **Edit User List**. The Edit User List screen appears, as shown in [Figure 10-2](#).

Figure 10-2 WebEx Site Administration - Edit User List

The screenshot shows the 'Edit User List' interface in the WebEx Site Administration. The page includes a search bar for user name and email, a 'Show active accounts only' checkbox, and a 'View' dropdown set to 'All Accounts'. Below this is an alphabetical index and a table of users. The table has columns for 'Active', 'Name', 'Email', 'User Name', 'Create Time', and 'Session Type'. The 'Session Type' column is further divided into 'PRO', 'AUTO', and 'PRO'. A red box highlights the 'PRO' header in the Session Type column, and a red arrow points to the 'PRO' checkbox in the first row. The 'Edit User List' link in the left sidebar is also highlighted with a red box.

Active	Name	Email	User Name	Create Time	PRO	AUTO	PRO
<input checked="" type="checkbox"/>	Name A	namea@yourcompany.com	namea	2/19/10 11:55 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Name B	nameb@yourcompany.com	nameb	2/18/10 10:38 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Name C	namec@yourcompany.com	namec	2/18/10 10:51 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Name D	named@yourcompany.com	named	2/18/10 10:42 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Name E	namee@yourcompany.com	namee	4/8/10 4:07 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Step 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 Figure 10-2.)

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 10-3. Locate the column that brings up the session type feature list titled “Supported Features in TelePresence”; this is the Meeting Center TelePresence session type.



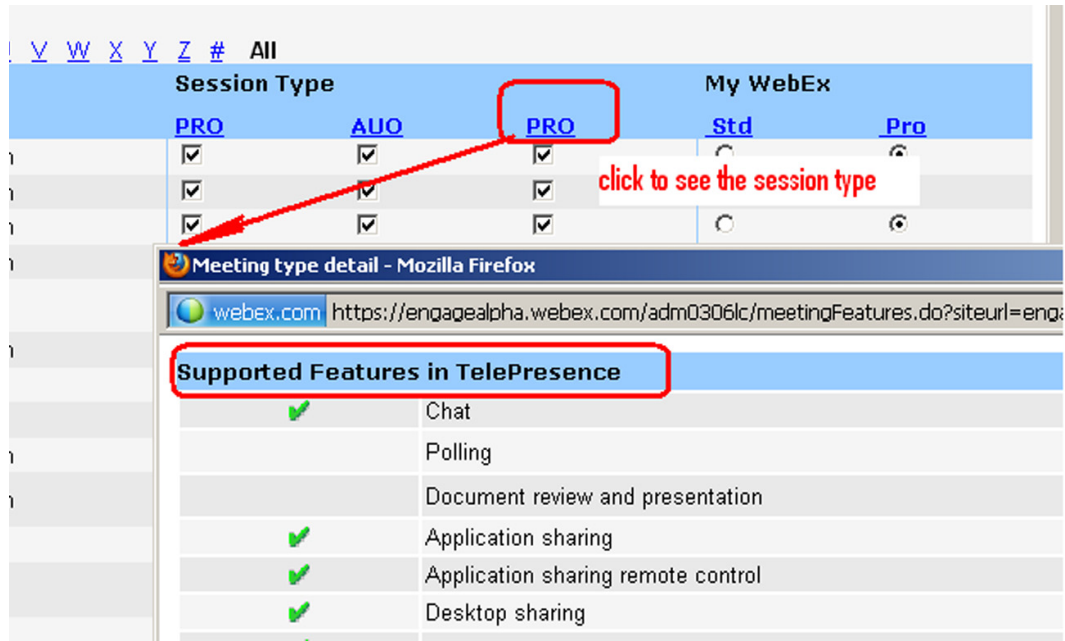
Note The number of session type columns is determined by how many session types the WebEx site supports.

Step 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.

Step 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 WebEx Enabled TelePresence.

Figure 10-3 Supported Features in TelePresence



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 OneTouch meetings. If this site is an existing site updated to WebEx Enabled TelePresence, 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:

- Step 1** Locate the user entry and click on it to open the Edit User window for that account.
- Step 2** Scroll down to the Privileges section. The assigned session types are shown in the Session Type Allowed box, as shown in [Figure 10-4](#).

Figure 10-4 Session Types Allowed

Privileges:	
Service	Session Type Allowed
	Select All Clear All
Meeting Center	<input checked="" type="checkbox"/> PRO: Meeting Center Pro meeting <input checked="" type="checkbox"/> AUO: WebEx Personal Conference <input type="checkbox"/> PRO: Meeting Center Pro Eval 4x20 <input checked="" type="checkbox"/> PRO: Meeting Center TelePresence

Step 3 Required. Check the box for **PRO: Meeting Center TelePresence**, as shown circled in red in Figure 10-4.

Step 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.



Tip

To upgrade any features, notify your Cisco WebEx business contact.

Network-Based Recording of WebEx Enabled TelePresence Meetings

With release T29 of WebEx, meeting organizers can now record WebEx Enabled TelePresence 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.

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.

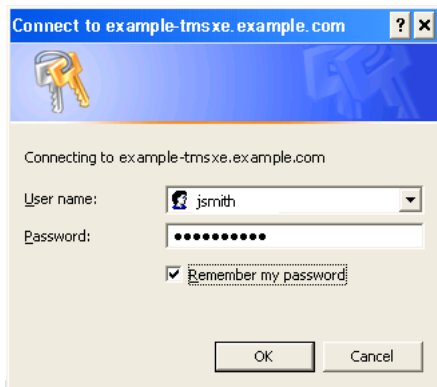
To install the WebEx Productivity Tools, users must do the following:

-
- Step 1** Open a browser and go your WebEx site.
- Step 2** Click **My WebEx**.
- Step 3** Log in to your account.
- Step 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.
- Step 5** In the left-hand navigation bar, click **Productivity Tools Setup**.
- Step 6** The **ptools.msi** file is downloaded to your computer.
- Step 7** After the download is complete, open **ptools.msi** and follow the on-screen instructions to install the WebEx Productivity Tools.
- Step 8** During the installation you must log in to your WebEx site.

Figure 10-5 WebEx Productivity Tools Login

- Step 9** Enter your WebEx Site URL, User Name, Password and click **Login**.

After logging in, the WebEx Productivity Tools communicates with the server and then your are asked to log into TMSXE.

Figure 10-6 TMSXE Login

- Step 10** Enter your TMSXE User name and Password and click **OK**.
- Step 11** When the message “WebEx Productivity Tools are installed” appears, click **OK**.
- Step 12** Close the Productivity Tools window.

You can now open Microsoft Outlook and schedule WebEx Enabled TelePresence 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:

- Step 1** Open a browser and go to your WebEx site.
- Step 2** Click **My WebEx**.
- Step 3** Enter your WebEx username and password and click **Log In**.

If you are presented with an option to download the WebEx Productivity Tools and you have already downloaded them, click **Later**. If you wish download and install them now, refer to step 4 of [Installing the WebEx and TelePresence Integration to Outlook, page 10-6](#)

The My WebEx Meetings page appears.

In the right corner of the page, the current language and time zone settings are displayed.

- Step 4** To change the language and time zone, click on the link that displays either the current language or time zone.
- The Preferences page appears.

- Step 5** Using the **Time zone** and **Language** menus, select the time zone and language you wish to use for your WebEx Enabled TelePresence meetings.
- Step 6** Click **OK**.
-

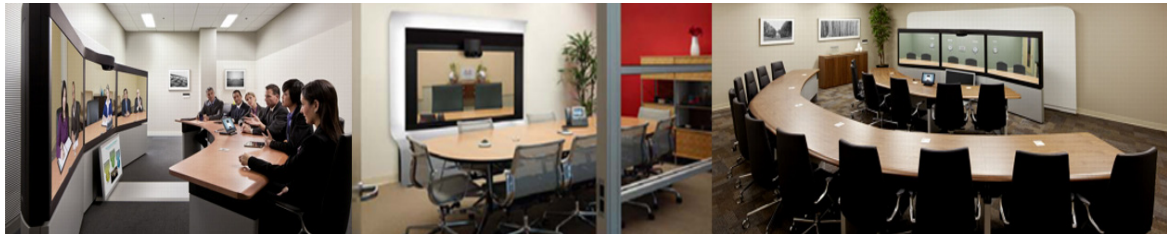
Configuring TSP Audio for a User's WebEx Account

Meeting organizers who need to schedule WebEx Enabled TelePresence meetings that use TSP audio, must add TSP audio provider information to their account.

For details, refer to [Configuring TSP Audio for the Meeting Organizer, page 9-11](#).

Where to Go Next

For complete information about managing your Cisco WebEx Administration Site account, refer to the Help on your WebEx site.



CHAPTER 11

Scheduling Cisco WebEx Enabled TelePresence Meetings

Revised: November 2013

Contents

This chapter provides a background on how to schedule Cisco WebEx Enabled TelePresence meetings, with tips and known issues. It contains the following sections:

- [Introduction, page 11-2](#)
- [Scheduling WebEx Enabled TelePresence Meetings in Cisco TMS, page 11-3](#)
- [Information, Tips and Known Issues About WebEx Enabled TelePresence Meetings, page 11-5](#)

Introduction

This chapter provides an overview of how to schedule WebEx Enabled TelePresence meetings using TMS and useful information, tips and known issues about WebEx Enabled TelePresence meetings.

In addition to scheduling using TMS, there are up to 3 additional ways to schedule a WebEx Enabled TelePresence meeting:

- Using the Cisco WebEx and TelePresence Integration to Outlook

With the WebEx and TelePresence Integration to Outlook, users can schedule WebEx Enabled TelePresence meetings directly from Microsoft Outlook for Windows. Advanced options like adding external video and audio dial-in participants are also available.

For scheduling information, refer to the [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 WebEx Enabled TelePresence 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 is 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 WebEx Enabled TelePresence Meetings 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 Cisco WebEx Enabled TelePresence Meeting:

- Step 1** Log in to Cisco TMS.
- Step 2** Go to **Booking > New Conference**.

Figure 11-1 Cisco TMS New Conference page

- Step 3** For Title, enter a conference title. It will be displayed in all Cisco TMS interfaces, and in email notifications about the meeting.
- Step 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.

- Step 5** Set the **Start Time** and the **End Time** or **Duration** for the meeting.
- Step 6** Make sure **Include WebEx Conference** is checked.
- Step 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.

Step 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.

Step 9 Optionally, add notes about the meeting in Conference Information, which will appear in the meeting invitation.

Step 10 In the Participant tab, click **Add Participant** and a new window will appear.

- 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.
- 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.
- Hover over any system, or the blocks in the planner view, for additional detail about the system or scheduled meeting.

Step 11 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.

Step 12 Use the External tab to add systems not managed by Cisco TMS, for example endpoints in other organizations, or telephone participants.

- For dial-out participants, enter their contact information, and Cisco TMS will automatically connect them to the conference at the scheduled time.
- 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.

Step 13 When all participants have been added, click **OK**.

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.

Step 14 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.

- Step 15** 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 emails 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:
 - 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.
 - Edit the conference settings to try to resolve the issue and try saving the conference again.
- Step 16** After successfully scheduling your meeting, invite people to the meeting using your calendar application.

For information about the Cisco WebEx Enabled TelePresence meeting experience, see [Cisco WebEx Enabled TelePresence Experience, page 1-1](#).

Information, Tips and Known Issues About WebEx Enabled TelePresence Meetings

The following section contains useful information, including tips and known issues relating to Cisco WebEx Enabled TelePresence meetings. The information is divided into sections corresponding to each product that is part of the Cisco WebEx Enabled TelePresence Solution.

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.
- Starting a meeting early is supported for both TelePresence and WebEx using the Default Setup Buffer setting when scheduling the meeting.

**Note**

Setup (and teardown) buffers are not supported when using Smart Scheduler, the WebEx and TelePresence Integration to Outlook, or any other client that uses the TMS booking API.

- 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 TMS.

If the original meeting is modified later in TMS, the meeting information in TMS will fall out of sync with the meeting organizer's Outlook calendar. The reason for this is that 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.

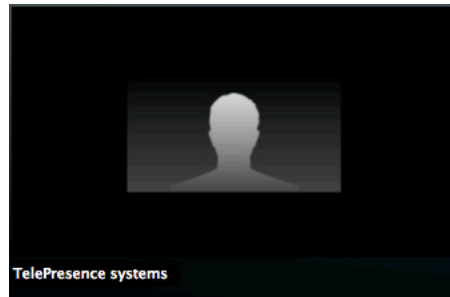
TMSXE

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

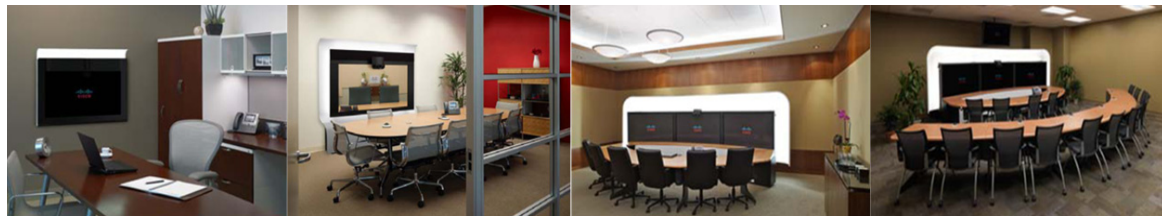
- A black silhouette is shown for a WebEx user when they do not have their camera on or when they do not have enough bandwidth to send video using their WebEx client.
- In the WebEx Meeting Center, all TelePresence endpoints are displayed as one WebEx participant called “TelePresence systems” both in 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 in [Figure 2](#).

Figure 2 “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.
- Audio quality can be bad for WebEx participants using Computer Audio when attending using the WebEx Meeting Center client on Windows or Mac. Cisco recommends users to call in with a phone using the audio conference number for the meeting.
- 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 user can start the 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, a non-Host has to 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.

- The link bandwidth between MCU and WebEx is set by the WebEx client with the lowest bandwidth. The bandwidth of the link 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 for all participants will be 360p. When that participant leaves the meeting, if all other participants are capable of a higher bandwidth, like 720p, the bandwidth will go up for all participants.



CHAPTER 12

Troubleshooting

Revised: October 2013

Contents

- [Verifying and Testing](#), page 12-1
- [Troubleshooting Tips](#), page 12-1
- [Managing System Behavior](#), page 12-10

Verifying and Testing

- [Cisco WebEx Site Administration Online Help](#), page 12-1

Cisco WebEx Site Administration Online Help

For complete information about using Cisco WebEx Site Administration, go to the Cisco WebEx Site Administration Help:

-
- Step 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*
- Step 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 Cisco WebEx Enabled TelePresence meeting:

- [Problems with Scheduling a Meeting](#), page 12-2
- [Problems with Starting or Joining a Meeting](#), page 12-3

- [Problems During a Meeting, page 12-4](#)
- [Problems with a TSP Audio Meeting, page 12-7](#)
- [Managing System Behavior, page 12-10](#)

Problems with Scheduling a Meeting

This section describes possible issues the meeting organizer may experience when scheduling a meeting using Cisco TMS.

Refer to troubleshooting information in [Table 12-1](#) to solve common problems that prevent meetings from being scheduled correctly.

Table 12-1 **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: Assigning the Meeting Center TelePresence Session Type, page 10-3 .
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: <ul style="list-style-type: none"> • 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”.

Table 12-1 Problems with Scheduling Meetings (continued)

Problem or Message	Possible Causes	Recommended Action
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 WebEx Enabled TelePresence.
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 WebEx Enabled TelePresence 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.
I don't 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 [Table 12-2](#) to solve common problems that prevent participants from starting or joining meetings.

Table 12-2 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.
TelePresence meeting didn't start early (Early Meeting Start) didn't work	Cisco TMS scheduled meeting doesn't support early start. Endpoint must wait until meeting has started to dial in.	Check Setup Buffer and Tear Down Buffer settings

Table 12-2 **Problems with Starting or Joining Meetings (continued)**

Problem or Message	Possible Causes	Recommended Action
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 hasn't started yet. Cisco TMS scheduled meeting doesn't 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.
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.	<ul style="list-style-type: none"> Do not use the same WebEx host ID to join multiple meetings at the same time. Only one WebEx Enabled TelePresence meeting can be run per host at a time.

Problems During a Meeting

This section describes possible issues meeting participants may experience during a meeting.

Refer to troubleshooting information in [Table 12-3](#) to solve common problems during the meeting.

Table 12-3 **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	<ul style="list-style-type: none"> • 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.
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	<ul style="list-style-type: none"> • -
Don't see video on WebEx	WebEx participant does not enable video. WebEx participant has a problem with their camera.	<ul style="list-style-type: none"> • Make sure TelePresence and WebEx calls are connected. • Check to see if participants who joined TelePresence are sending video.
Don't see video on TelePresence	-	<ul style="list-style-type: none"> • Check to see if WebEx users have joined and are sending video.
Don't hear audio on WebEx	-	<ul style="list-style-type: none"> • 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	-	<ul style="list-style-type: none"> • 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	-	<ul style="list-style-type: none"> • Check TelePresence statistic for content channel status. • Check to see if WebEx users can see content from each other.

Table 12-3 **Problems During the Meeting (continued)**

Problem or Message	Possible Causes	Recommended Action
Don't see presentation from TelePresence side on WebEx side	-	<ul style="list-style-type: none"> • 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	-	<ul style="list-style-type: none"> • Contact the WebEx administrator for assistance.
Don't see presentation from TelePresence side on TelePresence side	-	<ul style="list-style-type: none"> • Check TelePresence call statistics to see if content channel is established. • Try to stop the restart sending content.
Presentation is displayed in main video	-	<ul style="list-style-type: none"> • Check current call statistics for content channel. • Check to see if the SIP call encrypted.
Poor quality video from WebEx participants on TelePresence side	-	<ul style="list-style-type: none"> • Check network bandwidth for possible poor network connection.
Poor quality video from TelePresence participants on WebEx side	Poor network connection	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • -
Active speaker does not switch in	-	<ul style="list-style-type: none"> • 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.	<ol style="list-style-type: none"> 1. WebEx site administrator not configured properly. 2. Audio call failed. 3. If the MCU sends the wrong participant ID. 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Check the bandwidth between TelePresence and WebEx.
Video from a WebEx participant frozen	Possible network issue.	<ul style="list-style-type: none"> • Check the bandwidth between TelePresence and WebEx.
Meeting ends unexpectedly	-	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Check Cisco TMS booking list to confirm.

Problems with a TSP Audio Meeting

This section describes possible issues with a meeting that uses TSP audio.

Refer to troubleshooting information in [Table 12-4](#) to solve common problems with TSP audio meetings.

Table 12-4 *Problems with a TSP Meeting*

Problem or Message	Possible Causes	Recommended Action
<p>TelePresence joins audio of host's previously scheduled meeting that had run beyond the scheduled end time.</p>	<p>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.</p> <p>Example:</p> <p>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.</p> <p>This may be a pretty well understood circumstance for customers due to the way TSP Audio works.</p>	<ul style="list-style-type: none"> • Have TelePresence recite audio prompt after joining the TSP audio. "Cisco Telepresence is now in the audio conference" (or similar) <p>Note Using API method does not resolve this.</p>
<p>TelePresence joins audio of host's previously scheduled meeting where the host had exited with the "keep audio conference running" option.</p>	<p>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.</p> <p>This may be a pretty well understood circumstance for customers due to the way TSP Audio works.</p>	<ul style="list-style-type: none"> • Have TelePresence recite audio prompt after joining the TSP audio. "Cisco Telepresence is now in the audio conference" (or similar). <p>Note Using API method does not resolve this.</p>

Table 12-4 *Problems with a TSP Meeting (continued)*

Problem or Message	Possible Causes	Recommended Action
<p>“Host private conference code” can break DTMF dumb dial entry method in some cases (dial in as host + host has already dialed in).</p>	<p>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).</p>	<ul style="list-style-type: none"> • 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.
<p>MCU/TelePresence server is unable to dial out.</p>	<p>PSTN calls may not be configured to pass through a PSTN gateway to WebEx. Outbound dialing from VCS may not be properly configured.</p>	<ul style="list-style-type: none"> • Configure calls to pass through a PSTN Gateway to WebEx. • Verify the outbound dialing configuration for VCS and MCU/TelePresence Server.

Table 12-4 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).	<p>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.</p> <p>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].</p>	<ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 1. TelePresence starts TelePresence meeting. 2. TelePresence starts WebEx meeting. 3. WebEx sends W2A_CreateConference to TSP. 4. TSP sends A2W_RspCreateConference to WebEx (this would contain the TP dial string). 5. WebEx sends dial string to MCU. 6. MCU dials into the TSP bridge. <p>The TSP API and TSP Server would need to change (among other components, of course).</p>
The TSP Audio account info, used by the MCU dial string, is obsolete.	<p>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.</p>	<ul style="list-style-type: none"> • 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 [Table 12-5](#) to solve common problems with TelePresence Server and MCU.

Table 12-5 Problems with TelePresence Server and MCU

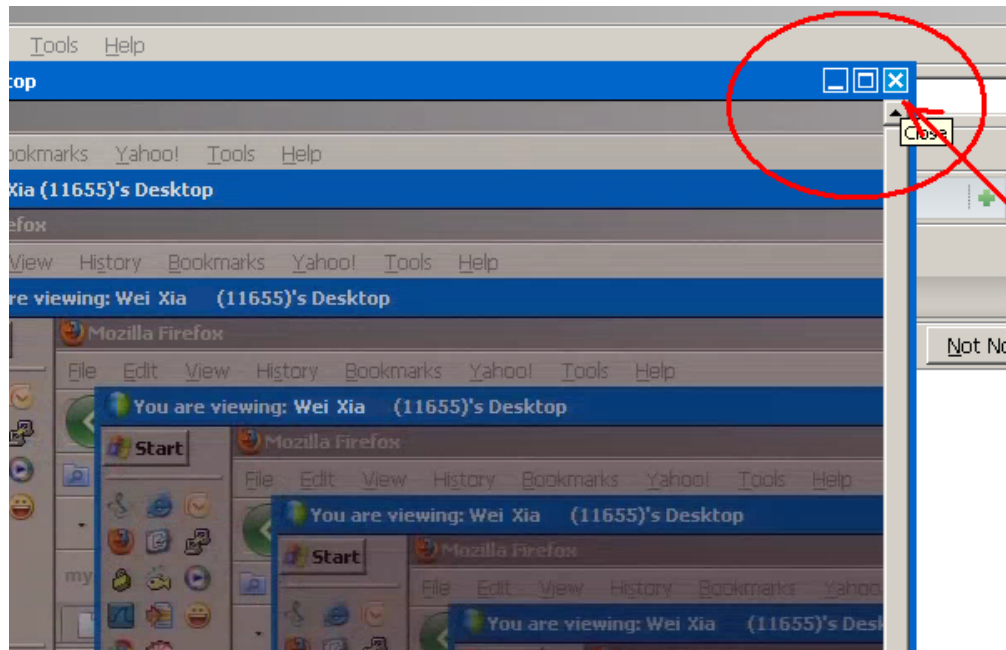
Problem or Message	Possible Causes	Recommended Action
MCU/TelePresence Server disconnects shortly after connecting to WebEx. A SIP Bye message is received from the WebEx cloud.	WebEx host joins a meeting while already joined to a meeting of which they are also the host.	<ul style="list-style-type: none"> Do not use the same WebEx host ID to join multiple meetings at the same time. <p>Note Only one WebEx Enabled TelePresence meeting can be run per host at a time.</p>

Managing System Behavior

- Managing the Cisco WebEx Video View Window, page 12-10

Managing the Cisco WebEx Video View Window

A window cascading effect can occur if you plug in the presentation cable 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 12-1](#).

Figure 12-1 Cascading Cisco WebEx Video View Window

254263