



## **Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide (TMS 15.0 - WebEx Meeting Center WBS30)**

**First Published:** 2016-05-02

**Last Modified:** 2017-04-24

### **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

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.

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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://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. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### About CMR Hybrid 1

Cisco TelePresence Meetings 1

Cisco Webex Meetings 1

Supported Features 2

Escalated/Instant Conferencing 4

Feature Limitations 4

Related Documents 4

---

### CHAPTER 2

#### Planning 7

Understanding How CMR Hybrid is Deployed 7

Cisco TMS Scheduling Role 8

TelePresence Server and MCU Roles 8

Ports and Protocols Used in CMR Hybrid 8

Understanding Scheduling Flow 9

Scheduling with the Cisco WebEx and TelePresence Integration to Outlook 10

Scheduling with the Cisco Smart Scheduler 12

Scheduling with the Cisco WebEx Scheduling Mailbox 14

Differences When Scheduling TelePresence Conductor-Managed Bridges 15

Understanding Call Flow 18

SIP Audio Call Flow 19

TSP Audio Call Flow with API Command to Unlock Waiting Room 21

TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host 22

WebEx Audio (PSTN) Call Flow 24

Server and Site Access Checklist 25

---

### CHAPTER 3

#### Deployment Options 29

SIP Video, Presentation, and Audio in a Unified CM-centric Deployment 29

SIP Video, Presentation, and PSTN Audio in a Unified CM-centric Deployment 30

SIP Video, Presentation, and Audio in a VCS-centric Deployment	32
SIP Video, Presentation, and PSTN Audio in a VCS-centric Deployment	32

---

## CHAPTER 4

### Requirements 35

CMR Hybrid Prerequisites	36
CMR Hybrid Product and Service Requirements	36
CMR Hybrid CPU Requirements	40
CMR Hybrid Network Requirements	40
IP Ranges, Protocols and Ports Used by CMR Hybrid	40
Conference Bridges	42
Multiparty Licensing	42
TelePresence Conductor	43
Default SIP TCP Timeout in Cisco Expressway / Cisco VCS	43
Security and Encryption	43
Configuration Summary	44
Resilience and Clustering	44
SIP Early Offer Messaging	45
Bridge Pools and Service Preferences	45
Content Channel	46
H.323 Interworking	46
Microsoft Lync 2013 Interoperability	46
Recommended Screen Resolutions for Presentation Sharing	46
Network and Client Restrictions that Affect Video in the WebEx Client	47

---

## CHAPTER 5

### Set Up the Solution Components 49

Set Up the Conference Bridges, TelePresence Conductor, and Unified Communications Manager	49
Enable Personal CMRs	50
Role of Personal CMRs in Multiparty Licensing	50
Personal CMR Templates and Conductor Conference Templates	51
Enable Personal CMRs Task Flow	51
Create a TelePresence Conductor User with API Access	52
Add the TelePresence Conductor API User to Cisco TMSPE	53
Enable WebEx for Personal CMRs	53
Create CMR Templates	54

Apply CMR Templates to Groups	54
Enable Monitoring for Personal CMRs	54
Synchronize CMRs	54
Manage Multiparty Licensing	55
Enable Multiparty Licensing	55
Apply Licenses to Users	56
Change the Licensing Mode	56
Manually Synchronize Licenses	57
Monitor License Use	57

---

## CHAPTER 6

### Connect Cisco TelePresence Conductor to Call Control 59

Connect TelePresence Conductor to Cisco Unified Communications Manager	59
Connect TelePresence Conductor to Cisco VCS	60

---

## CHAPTER 7

### Configure Bridge Scheduling 61

How Bridges are Scheduled in CMR Hybrid	61
Limitations	62
Requirements	63
Requirements for Dedicated Bridge Scheduling	63
Configurations for Scheduled Conferencing	64
Shared Bridges	64
Alternative Options (Dedicated Bridges)	64
Enable Scheduling in TelePresence Conductor and Cisco TMS	67

---

## CHAPTER 8

### Configure Cisco MCU and TelePresence Server 71

MCU and TelePresence Server Overview	71
MCU Configuration Task Flow	72
Configure Content Mode for MCU	72
Set Video and Audio Codecs	73
Configure Automatic Content Handover	73
Configure the Default SIP Domain for TSP Audio	74
Automatically Make Content Channel Important	74
Configure Outgoing Transcoded Codec	75
Configure Adaptive Gain Control	75
Configure Audio Notifications	76

Configure Encryption	76
TelePresence Server Configuration Task Flow	77
Configure Locally Managed Mode	77
Configure Automatic Content Handover	78
Configure the Display Setting	78

---

## CHAPTER 9

### Configure Call Control 81

Call Control Overview	81
Cisco Expressway and TelePresence Configuration Tasks	82
Create a New DNS Zone	84
Configure Traversal Zones for MCUs	85
Configuring Cisco Unified Communications Manager	85
Cisco Unified Communications Manager Configuration Prerequisites	86
SIP Trunks Between Cisco Unified Communications Manager and Cisco Expressway-C or Cisco VCS Control	86
Configuring Early Offer for SIP Messaging	86
Scenario 1. Configuring Early Offer in a single Unified CM system	87
Scenario 2. Configuring Early Offer in a multi-cluster system (TelePresence Conductor connected to Unified Communications Manager SME)	87
Scenario 3. Configuring Early Offer in a multi-cluster system (TelePresence Conductor connected to Unified Communications Manager SME)	88
Configuring Early Offer (and fallback to Delayed Offer) for SIP trunks	88
Fallback to Delayed Offer	88
Endpoints	89
Configuring a Routing Rule for Bridges Trunked to Unified Communications Manager	89
Provisioning Endpoint Display Names	90
Provisioning Display Names on Unified CM	91
Users and Devices	91
Line	91
Set Display Names for Unified CM Registered Endpoints using Bulk Administration	91
Manually Set Display Names for Unified CM Registered Endpoints	92
Trunks	92
Provisioning Display Names on Cisco VCS	93
FindMe	93

Setting Caller ID Display Names for Cisco VCS Users	93
Setting Caller ID Display Names for Conference Rooms	94

---

## CHAPTER 10

<b>Configure Certificates on Cisco Expressway-E and Cisco VCS Expressway</b>	<b>95</b>
Supported Certificates	95
Certificate Configuration Tasks	96
Generate a Certificate Signing Request (CSR)	97
Install the SSL Server Certificate	97
Configure the Trusted CA List	98
Stack the Intermediate Certificate CA Certificate	99
Trusted CA Certificate List Configuration Tasks for Upgrades	100
Reset the Trusted CA Certificate List	100
Update Certificates on Cisco Expressway-E or VCS Expressway X8.5	101
Expiration Dates of VeriSign and QuoVadis Certificates	102
Add the Intermediate Certificate CA Certificate	102
Trusted CA Certificate List Configuration Tasks for New Installations	103
Add the DST Root Certificate	104
Update Certificates on Cisco Expressway-E or VCS Expressway X8.5	104
Expiration Dates of VeriSign and QuoVadis Certificates	105
Add the Root or Intermediate Certificate CA Certificate	105

---

## CHAPTER 11

<b>Configure Cisco TelePresence Management Suite</b>	<b>107</b>
Prerequisites	107
Configuring the Cisco WebEx Feature in Cisco TMS	108
Configuring WebEx Users in Cisco TMS	109
User Requirements for Scheduling WebEx-enabled Meetings	109
Configuring Automatic User Lookup from Active Directory	110
Configuring Active Directory Lookup in Cisco TMS	110
How WebEx Bookings Work	111
Configuring a Cisco CMR Hybrid User in Cisco TMS	111
Configuring Port Reservations for MCU and TelePresence Server in Cisco TMS	112
Enabling Port Reservations for MCU	112
Enabling Port Reservations for TelePresence Server	113
Configuring Hybrid Content Mode for MCU in Cisco TMS	113
Configuring Lobby Screen in Cisco TMS	114

How the Lobby Screen Affects the First TelePresence Participant in a Meeting if the WebEx Welcome Screen is Disabled	114
Configuring Conference Settings in Cisco TMS	115
Default Picture Mode	116
Conference Connection/Ending Options	116
Configuring Allow Early Join	117
Configuring Resource Availability on Extension	118
Configuring Single Sign On in Cisco TMS	118
Prerequisites	119
Configuring SSO in Cisco TMS	119
Generating a Certificate for WebEx	120
Using an Existing Certificate Signed by a Trusted Authority	120
If Private Key is Exportable	120
If Private Key is Not Exportable, but Key/Certificate Pair Available	121
If Private Key is Not Exportable or Available	121
Creating a Key/Certificate Pair Signed by a Certificate Authority	121
Creating a Self-signed Key/Certificate Pair	122
Using OpenSSL to Generate a Certificate	122
Enabling Partner Delegated Authentication on the WebEx Site	124
Enabling SSO in Cisco TMS	125
Supported Configurations for Scheduling on Behalf of the WebEx Host	126
Guidelines for Renewing Your PDA/SSO	127

---

## CHAPTER 12

Configure Cisco TelePresence Management Suite Extension for Microsoft Exchange	129
Prerequisites	129
Deployment Best Practices	129
Scheduling Options with Cisco TMSXE	130
Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook	130
Installing the Booking Service	130
Configuring IIS for HTTPS	131
Configuring the Server Certificate	131
Generating a CSR for IIS 7 (Windows Server 2008)	131
Installing the Public Root Certificate in IIS 7 (Windows Server 2008)	132
Installing the Intermediate CA Certificate (If Applicable)	132
Installing the SSL Server Certificate	132



Setting Up Communication Between Your WebEx Site and Cisco TMSXE	133
Configuring the Location Displayed for TelePresence Rooms in Outlook	133
Installing the WebEx and TelePresence Integration to Outlook	133
Configuring Cisco TMSXE for the WebEx Scheduling Mailbox	134
Configuring the WebEx Scheduling Mailbox in Microsoft Exchange	134
Adding the WebEx Mailbox to Cisco TMSXE	135
Additional Recommendations	135

---

## CHAPTER 13

### Configure TelePresence Management Suite Provisioning Extension 137

Prerequisites	137
Introduction	138
User Access to Cisco TMSPE	138
Creating a Redirect to Smart Scheduler	138
Access Rights and Permissions	138
Time Zone Display	139
How Smart Scheduler Works	139
Limitations	139

---

## CHAPTER 14

### Configure Audio 141

Prerequisites	141
Configuring SIP Audio for CMR Hybrid	142
Configuring the WebEx Site in Cisco TMS to Use SIP Audio	142
Enabling Hybrid Audio on the WebEx Site	143
Configuring PSTN Audio for CMR Hybrid	143
Configuring the WebEx Site in Cisco TMS to Use PSTN Audio	143
Enabling Hybrid Mode on the WebEx Site	144
Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx	144
Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco VCS	144
Configuring for ISDN Gateways	144
Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco Unified Communications Manager	145
Configuring TSP Audio for CMR Hybrid	145
Overview of CMR Hybrid with a WebEx Site Using TSP Audio	145
Prerequisites	146
How a TSP Meeting Works	147

Configuring TSP Audio for the Meeting Organizer	148
TSP Audio Account Prerequisites	148
Configuring the TSP Audio Account of the WebEx Host Account	148
Information about the CMR Hybrid Dial String Used for TSP Sites	149
DTMF Dial String Example	149
How the Dial String is Determined	149

---

## CHAPTER 15

<b>Integrate Cisco TelePresence with a Cisco WebEx Site Administration Account</b>	<b>151</b>
Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account	151
Configuring Cisco WebEx Site Administration for CMR Hybrid	151
Assigning the Meeting Center TelePresence Session Type	153
Support for Custom Session Types	153
Adding the Cisco TelePresence Session Type in the List of Users	154
Adding the Cisco TelePresence Session Type in the Edit User Screen	154
Network-Based Recording of CMR Hybrid Meetings	155
Installing the WebEx and TelePresence Integration to Outlook	155
Setting the Time Zone and Language Preferences for a User's WebEx Account	156
Configuring TSP Audio for a User's WebEx Account	157
Where to Go Next	157

---

## CHAPTER 16

<b>Manage CMR Hybrid Meetings</b>	<b>159</b>
Introduction	159
Scheduling a CMR Hybrid Meeting	160
Starting/Joining the Meeting	162
Share Cisco WebEx Presentations	162
Information, Tips and Known Issues About Meetings	163
Cisco TMS	163
MCU and TelePresence Server	163
Endpoints	164
Cisco TMSXE	164
WebEx	164

---

## CHAPTER 17

<b>Troubleshoot CMR Hybrid</b>	<b>165</b>
Verifying and Testing	165
Cisco WebEx Site Administration Online Help	165

Troubleshooting Tips	165
Problems with Scheduling a Meeting	166
Problems with Starting or Joining a Meeting	167
Problems During a Meeting	169
Tips for Troubleshooting Low Bandwidth with the WebEx Meeting Center Client on Windows or Mac	173
Problems with a TSP Audio Meeting	173
Problems with TelePresence Server and MCU	176
Managing System Behavior	176
Managing the Cisco WebEx Video View Window	176

---

## APPENDIX A

### Add Cisco Unified Communications Manager Normalization Scripts 179

Normalization Script Overview	179
Add the Scripts	180

---

## APPENDIX B

### Migration Paths 181

Migration Overview	181
Migration Prerequisites	182
Supported Software Versions for Migration	182
Migrate a Cisco Unified Communications Manager-only System to CMR Hybrid	183
Separate Audio and Video Endpoints	183
Migrate Cisco Unified Communications Manager and Cisco VCS to CMR Hybrid	184
Comparison of Endpoint Capabilities	184
Features and Version Dependencies	185
Associated Products, Versions, and Features	185

---

## APPENDIX C

### Set Up Cascading for Large-Scale or Critical Meetings 187

Cascading Overview	187
Process for CMR Conferences	188
Process for Scheduled Conferences	188





## CHAPTER

# 1

## About CMR Hybrid

---

- [Cisco TelePresence Meetings, page 1](#)
- [Cisco Webex Meetings, page 1](#)
- [Supported Features, page 2](#)
- [Escalated/Instant Conferencing, page 4](#)
- [Feature Limitations, page 4](#)
- [Related Documents, page 4](#)

## Cisco TelePresence Meetings

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

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

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

## Cisco Webex Meetings

Remote participants join the Cisco WebEx meeting by logging in to the Cisco WebEx Meeting Center Web and/or mobile applications. Content shared by a Cisco TelePresence participant is displayed automatically in the Meeting Center application, and WebEx participants can share their desktop or application with

Cisco TelePresence participants. By default, WebEx participants see the live video of the actively speaking Cisco TelePresence or WebEx participant.

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

When the first WebEx participant joins, "TelePresence systems" appears in the list of WebEx participants and in the row of WebEx participants in Full Screen view. This indicates that it is a Cisco CMR Hybrid meeting. Individual TelePresence users are not listed in the WebEx participants list. Instead, only "TelePresence systems" is listed and is displayed in the active speaker window when a TelePresence participant is the active speaker.

## Supported Features

CMR Hybrid provides the following key features:

- Scheduled and always-on personal Collaboration Meeting Room options
- Two-way video sharing with up to 1080p screen resolution between the WebEx application and telepresence devices
- Integrated audio and presentation sharing — including application and desktop content sharing capability for all users in a meeting
- Integrated roster for WebEx participants, including telepresence device display names
- Network-based recording of meetings including content share, chat and polling
- Integrated meeting scheduling using Cisco TelePresence Management Suite (Cisco TMS), which allows you to easily schedule CMR Hybrid meetings
- Secure call control and connectivity enabled by media encryption provided by Cisco Expressway-E or Cisco VCS Expressway
- Unified CM-centric and VCS-centric call control deployment options
- Management and conference resource allocation of conference bridges provided by Cisco TelePresence Conductor
- Interoperability with third-party telepresence devices
- Interoperability with Microsoft Lync clients

**Table 1: CMR Hybrid Features**

Supported Feature	Description
Audio	<p>TelePresence participants have two-way audio with the Cisco WebEx meeting participants using G.711 and G.722.</p> <p><b>Note</b> No presentation audio is sent from the Cisco WebEx side.</p>

Supported Feature	Description
Host	The MCU/TS dials in at the meeting start time automatically to connect all TelePresence participants. The MCU/TS becomes the host if the meeting organizer has not joined on WebEx yet. If the meeting organizer joins the meeting on WebEx before the scheduled start time, they become the host.
Scheduling	<p>Use Cisco TMS, the WebEx and TelePresence Integration to Outlook, Smart Scheduler, or WebEx Scheduling Mailbox or the WebEx web site 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 Collaboration Meeting Rooms (CMR) Hybrid meeting earlier than the scheduled time if you are the WebEx host. WebEx participants who try to join the WebEx meeting before the host, receive a message that the meeting has not started and they must wait to join until the scheduled start time or until after the WebEx host joins.</p> <p><b>Note</b> Only scheduled meetings are supported for Cisco Collaboration Meeting Rooms (CMR) Hybrid Interoperability; non-scheduled TelePresence participants who want to join a Cisco Collaboration Meeting Rooms (CMR) Hybrid meeting, must manually dial into the conference (MCU/TelePresence Server) bridge. The meeting organizer reserves ports for video dial-in participants when scheduling the meeting.</p> <p>See <a href="#">Cisco TelePresence Management Suite Administrator Guide</a> 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 TS/MCU transcodes the presentation and sends it to the WebEx cloud at 1024 x 768 resolution.</p>
Two-way Video	<p>Video from Cisco TelePresence endpoints is sent to Cisco WebEx participants and video from Cisco WebEx participants is sent to Cisco TelePresence endpoints.</p> <p>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 each TelePresence endpoint.</p> <p><b>Note</b> All CMR Hybrid meetings require the use of a Cisco TelePresence Server or MCU.</p>

# Escalated/Instant Conferencing

We do not support Multiway (the Cisco VCS method of escalated conferencing) in the primary deployment.

## Feature Limitations

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

## Related Documents

Related Topic	Link
Cisco TelePresence Conductor	<a href="#">Cisco TelePresence Conductor</a>
Cisco TelePresence Management Suite	<a href="#">Cisco TelePresence Management Suite</a>
(Optional) Cisco Expressway Series	<a href="#">Cisco Expressway Series</a>
Cisco TelePresence Video Communication Server (Cisco VCS)	<a href="#">Cisco TelePresence Video Communication Server</a>
Cisco TelePresence Video Communication Server (Cisco VCS)	<a href="#">Cisco TelePresence Video Communication Server</a>
Cisco Unified Communications Manager (Unified Communications Manager)	<a href="#">Cisco Unified Communications Manager</a>
Cisco TelePresence Server	<a href="#">Cisco TelePresence Server</a> <a href="http://www.cisco.com/c/en/us/support/conferencing/telepresence-server-on-multiparty-media-310/model.html">http://www.cisco.com/c/en/us/support/conferencing/telepresence-server-on-multiparty-media-310/model.html</a> <a href="http://www.cisco.com/c/en/us/support/conferencing/telepresence-server-on-multiparty-media-320/model.html">http://www.cisco.com/c/en/us/support/conferencing/telepresence-server-on-multiparty-media-320/model.html</a>
Cisco TelePresence MCU Series	<ul style="list-style-type: none"> <li>• <a href="#">MCU 5300 Series</a></li> <li>• <a href="#">MCU 4501 Series</a></li> <li>• <a href="#">MCU 4500 Series</a></li> <li>• <a href="#">MCU 4200 Series</a></li> <li>• <a href="#">MCU MSE Series</a></li> </ul>
Cisco WebEx Documentation	



Related Topic	Link
Information about how to use Cisco WebEx meeting features.	<ul style="list-style-type: none"><li>• Go to your Cisco WebEx site home page.</li><li>• Log into your Cisco WebEx Meeting Center account and click on Support &gt; User Guides in the left navigation pane.</li></ul>
Specifying Cisco TelePresence Integration options and managing your Cisco WebEx Site.	See <a href="#">Integrate Cisco TelePresence with a Cisco WebEx Site Administration Account</a> , on page 151.
Cisco Collaboration Meeting Rooms (CMR) Hybrid Documentation	
Information for meeting organizers on how to schedule CMR Cloud meetings	<a href="http://www.cisco.com/en/US/products/ps11338/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps11338/products_user_guide_list.html</a>





## Planning

---

- [Understanding How CMR Hybrid is Deployed, page 7](#)
- [Understanding Scheduling Flow, page 9](#)
- [Understanding Call Flow, page 18](#)
- [Server and Site Access Checklist, page 25](#)

## Understanding How CMR Hybrid is Deployed

The core elements of CMR Hybrid are:

- TelePresence Conductor
- TelePresence Server and/or Cisco TelePresence MCU Series conference bridges
- Cisco TMS

The TelePresence Conductor manages the conference bridges. SIP trunks connect the bridges to the TelePresence Conductor, which in turn is trunked to one or more call controllers. All XML RPC connections also route via the TelePresence Conductor. Cisco TMS provides conference management, including scheduling, provisioning and monitoring of conferences. XML RPC connections link Cisco TMS to the TelePresence Conductor.

The solution architecture is exclusively SIP. Conferencing with H.323 endpoints requires interworking by a Cisco VCS Control or Cisco Expressway-C.

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

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

The supported deployment models are described in the section: [Deployment Options, on page 29](#).

## Cisco TMS Scheduling Role

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

## TelePresence Server and MCU Roles

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

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

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

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

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

## Ports and Protocols Used in CMR Hybrid

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

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

\*For a complete list of WebEx IP subnets, refer to article WBX264, in the [WebEx Knowledge Base](#).

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

**Important**

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

## Understanding Scheduling Flow

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

- [Scheduling with the Cisco WebEx and TelePresence Integration to Outlook](#), on page 10
- [Scheduling with the Cisco Smart Scheduler](#), on page 12
- [Scheduling with the Cisco WebEx Scheduling Mailbox](#), on page 14

**Note**

Multiple deployments are possible at the same time. For example, when using Smart Scheduler, if TMSXE 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

Cisco WebEx and TelePresence Integration to Outlook Scheduling Flow

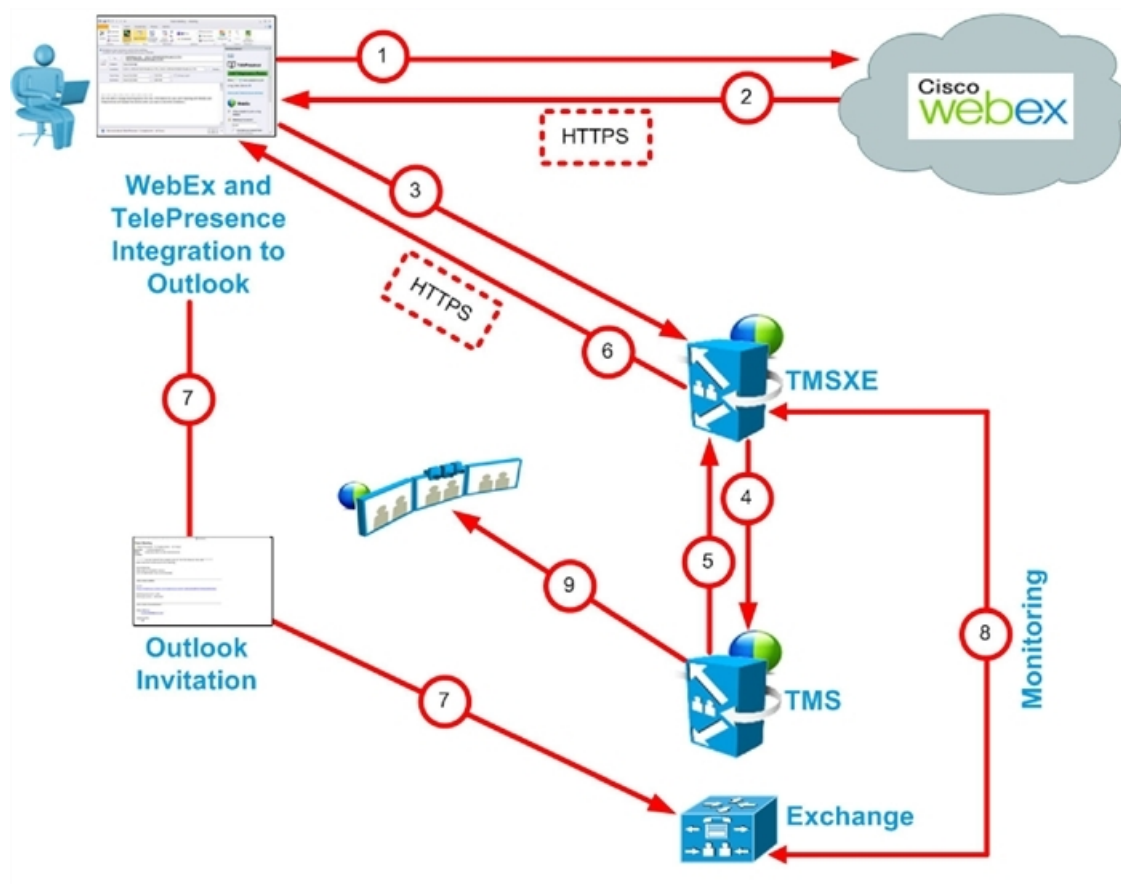


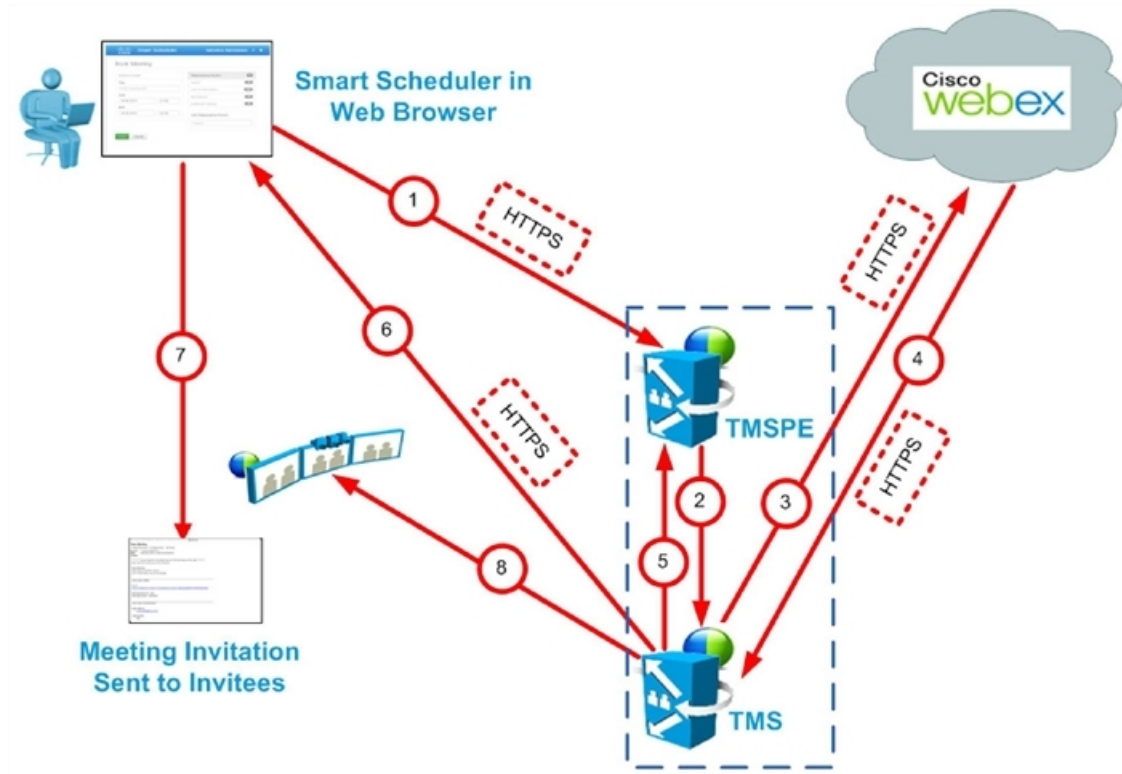
Table 2: Cisco WebEx and TelePresence Integration to Outlook Scheduling Steps

Step #	Description
1	User books meeting with Cisco WebEx and TelePresence Integration to Outlook. Adds users Adds rooms Meeting request is sent to WebEx and books the WebEx portion of meeting.

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

# Scheduling with the Cisco Smart Scheduler

## Cisco WebEx Smart Scheduler Scheduling Flow



**Table 3: Cisco Smart Scheduler Scheduling Steps**

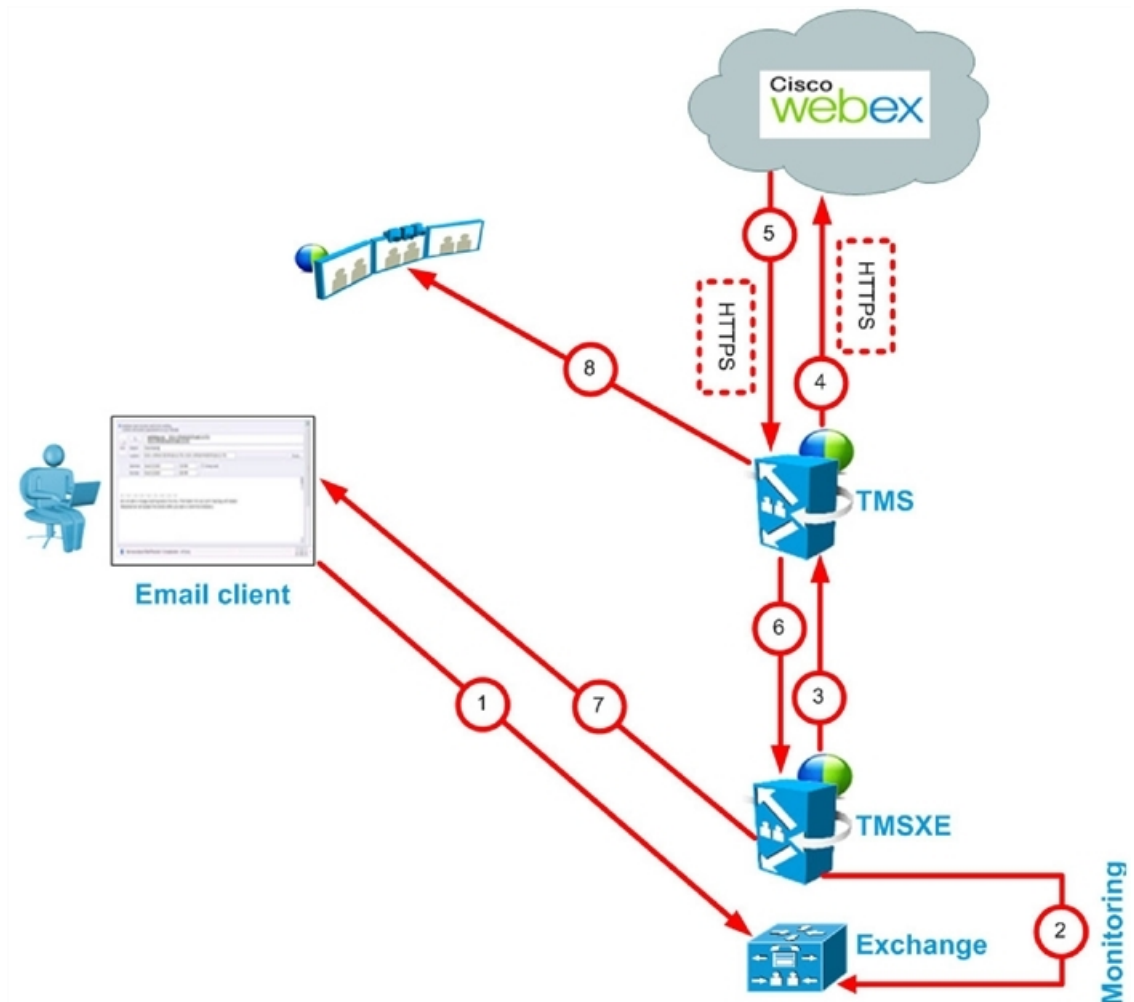
Step #	Description
1	User books meeting with Smart Scheduler. Adds rooms Adds WebEx Clicks Save.
2	TMSPE sends a booking request to TMS.
3	TMS sends booking request to WebEx. WebEx books WebEx portion of meeting.



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

# Scheduling with the Cisco WebEx Scheduling Mailbox

## Cisco WebEx Scheduling Mailbox Scheduling Flow



**Table 4: Cisco WebEx Scheduling Mailbox Scheduling Steps**

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

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

## Differences When Scheduling TelePresence Conductor-Managed Bridges

Before moving to a TelePresence Conductor scheduling deployment, note the following differences between scheduling direct-managed bridges and bridges managed by TelePresence Conductor.

**Table 5: Differences when scheduling TelePresence Conductor-managed bridges**

	Direct-managed	TelePresence Conductor-managed
Booking	<ul style="list-style-type: none"> <li>• Conference configurations can be set per conference, over-riding default conference settings.</li> <li>• Cisco TMS chooses the SIP URI to provide the dial-in number for the conference.</li> <li>• Can be added to Cisco TMS participant and conference templates.</li> <li>• No option to overbook bridge resources.</li> </ul>	<ul style="list-style-type: none"> <li>• Some conference configurations are set on the TelePresence Conductor conference template, and cannot be changed during booking.</li> <li>• Users can input the variable part of the alias during booking to create the dial-in number for the conference.</li> <li>• Cannot be added to Cisco TMS participant and conference templates.</li> <li>• Overbooking of bridge resources: Using the service preference capacity adjustment feature, you can configure Cisco TMS to allow overbooking of the actual resources available on the bridges in the pools associated with the service preference. By doing this, you allow for the case where users unnecessarily book more ports than they need for conferences, thereby freeing up unused resources for other users.</li> </ul>

	Direct-managed	TelePresence Conductor-managed
Cascading	<ul style="list-style-type: none"> <li>• Does not support cascaded TelePresence servers.</li> <li>• Cisco TMS decides whether to cascade MCUs when routing conferences.</li> <li>• Cisco TMS cannot create a cascade after the conference has started if more participants join than the capacity on the hosting MCU(s)</li> <li>• More functionality in Conference Control Center for example, moving participants from one cascaded MCU to another.</li> <li>• Cascading is selected using the Distribution options when booking a conference.</li> <li>• Cascading is not possible when booking using clients that use Cisco TMS Booking API (Cisco TMSBA) for example: Microsoft Outlook and Smart Scheduler.</li> </ul>	<ul style="list-style-type: none"> <li>• Supports cascaded TelePresence Servers.</li> <li>• TelePresence Conductor cascades the bridges.</li> <li>• TelePresence Conductor can cascade on the fly if more participants join than the initial capacity of the hosting bridge(s).</li> <li>• No functionality in Conference Control Center, except visibility of which bridge a participant is connected to.</li> <li>• You have to select an alias that supports cascading when booking the conference.</li> <li>• Cascading is possible when booking using clients that use Cisco TMS Booking API (Cisco TMSBA) for example: Microsoft Outlook and Smart Scheduler.</li> </ul>
Conference Control Center	Full functionality dependent on the bridge type hosting the conference.	<p>The following functionality is not available for conferences hosted on a TelePresence Server managed by TelePresence Conductor:</p> <ul style="list-style-type: none"> <li>• Video protocol</li> <li>• Audio protocol</li> <li>• Encryption status</li> <li>• Number</li> <li>• Participant audio level</li> <li>• Video Resolution</li> <li>• Duo Video Status</li> <li>• Snapshots</li> </ul>

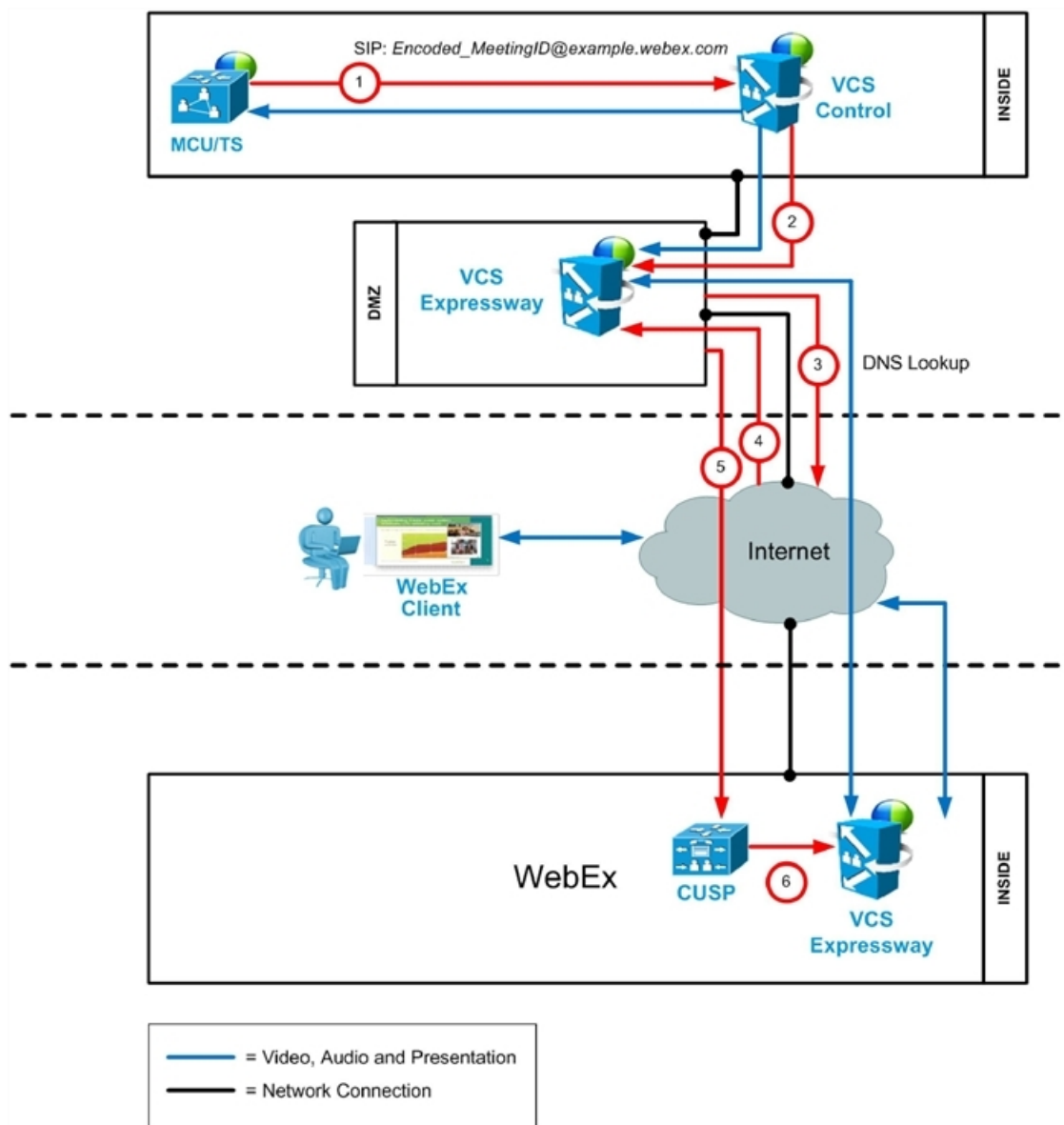
	Direct-managed	TelePresence Conductor-managed
Reporting	Full functionality	<ul style="list-style-type: none"> <li>• Call Detail Records (CDRs) from TelePresence Conductor-managed conference bridges will not contain any ConferenceIDs.</li> <li>• TelePresence Conductor itself does not feed back any conference CDRs to Cisco TMS. The bridges themselves will however, if added to Cisco TMS.</li> <li>• Depending on the call direction you might get incomplete CDR data, as dialing out can lead to incorrect data.</li> <li>• Bridge utilization reporting is not supported for conferences hosted on a TelePresence Conductor.</li> </ul>
Zones	Cisco TMS uses IP zones to ensure that systems uses bridges that are geographically closer.	Cisco TMS chooses which TelePresence Conductor to use based on IP zones but will disregard any IP zone information for the bridges themselves.

## Understanding Call Flow

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

- [SIP Audio Call Flow](#), on page 19
- [TSP Audio Call Flow with API Command to Unlock Waiting Room](#), on page 21
- [TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host](#), on page 22
- [WebEx Audio \(PSTN\) Call Flow](#), on page 24

## SIP Audio Call Flow



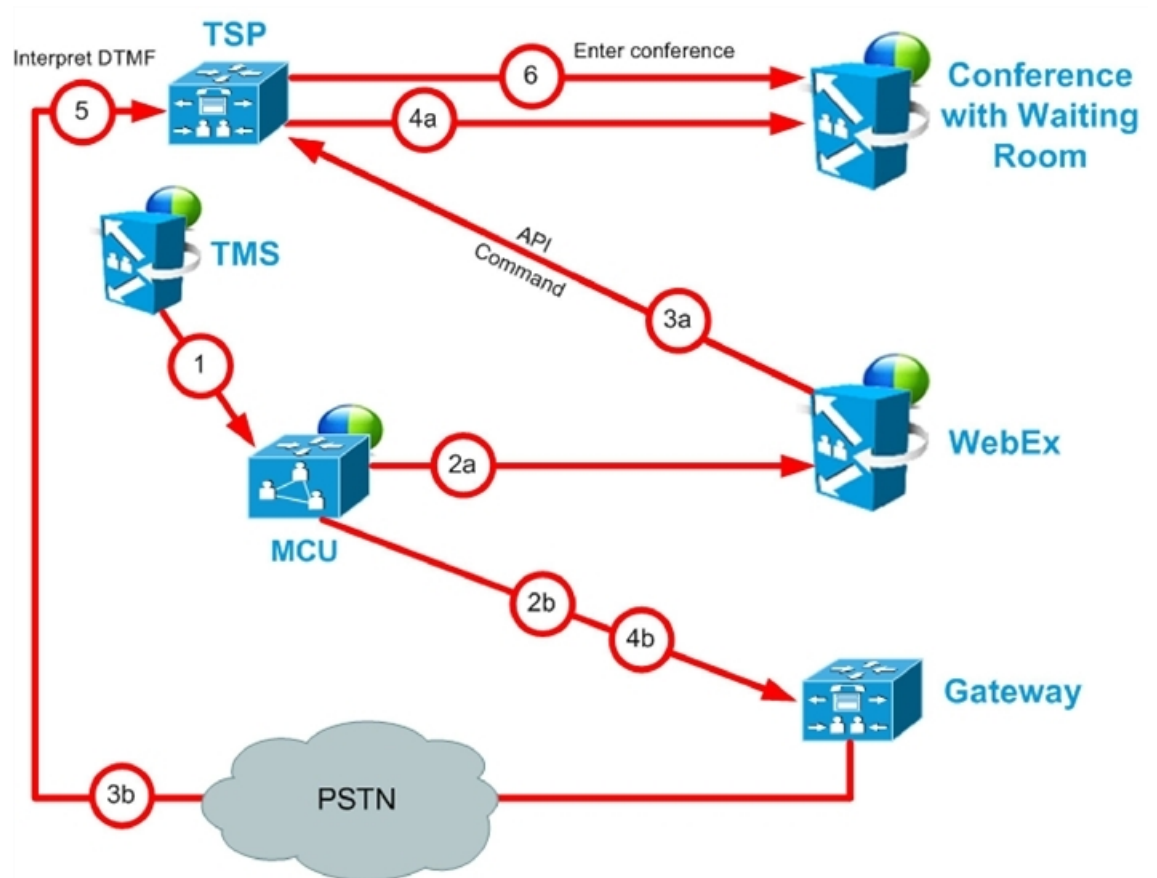
**Table 6: SIP Audio Call Flow Steps**

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

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



## TSP Audio Call Flow with API Command to Unlock Waiting Room

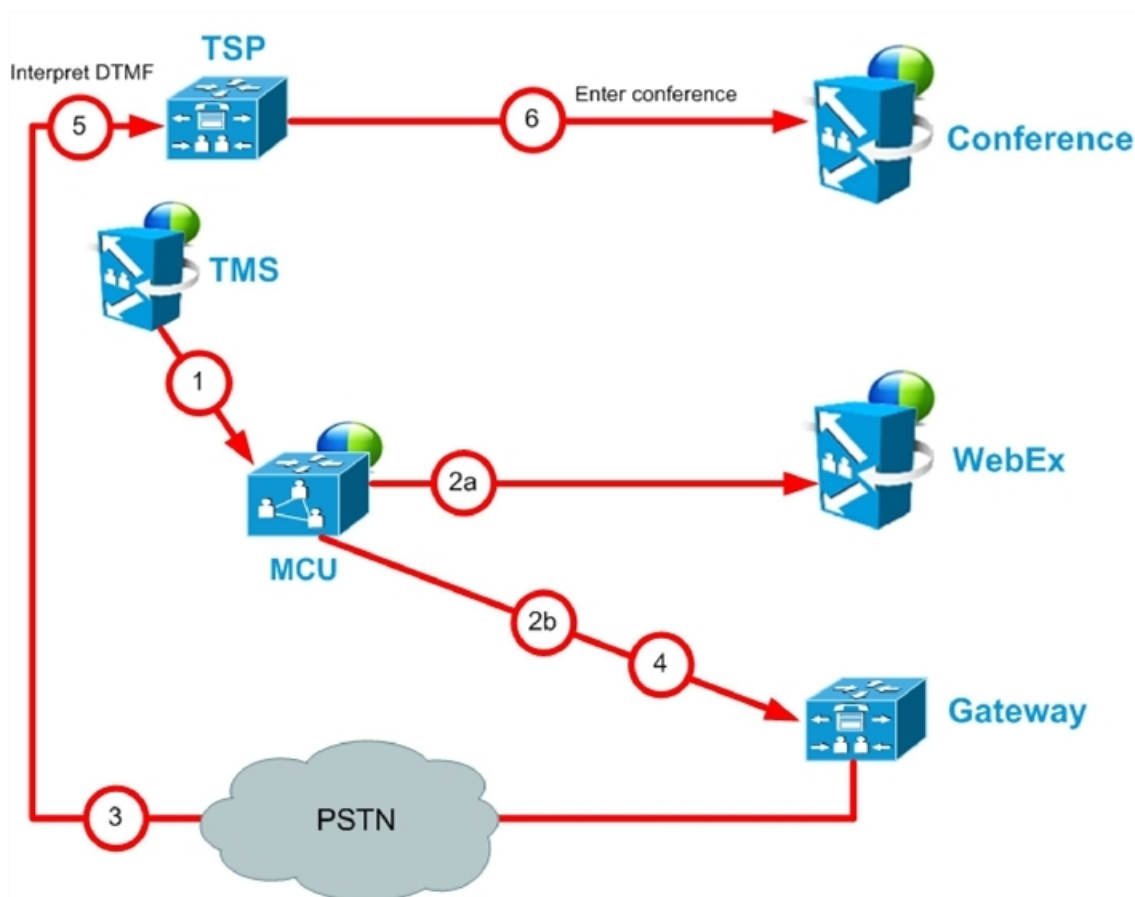


**Table 7: TSP Audio Call Flow with API Command to Unlock Waiting Room Steps**

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

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

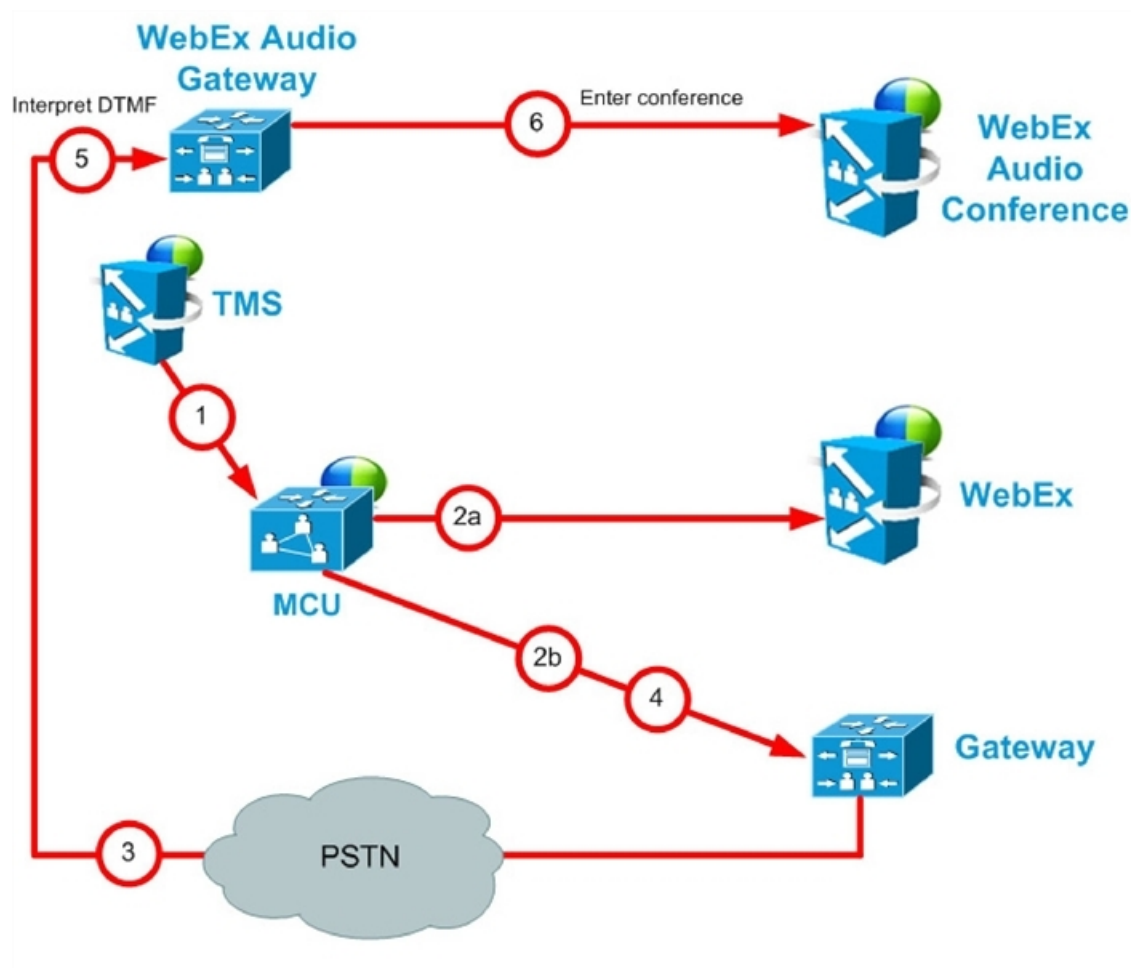
## TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host



**Table 8: TSP Audio Call Flow with Waiting Room and MCU/TelePresence Server as Host Steps**

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

## WebEx Audio (PSTN) Call Flow



**Table 9: WebEx Audio (PSTN) Call Flow Steps**

Step #	Description
1	TMS starts conference on MCU, providing it with the SIP URI, telephone number and DTMF string to dial into WebEx.
2a	MCU dials WebEx via SIP. (refer back to Understanding Cisco CMR Hybrid Call Flow [p.1] 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.

## Server and Site Access Checklist

*Table 10: Information you must have before configuring CMR Hybrid for the first time.*

What You Need	Description and Source	Done
WebEx Site URL	URL for the Cisco WebEx site. Provided by the Cisco WebEx Account Team. Example: <a href="https://example.webex.com/example">https://example.webex.com/example</a> See <a href="#">Configuring the Cisco WebEx Feature in Cisco TMS</a> , on page 108 for instructions.	
WebEx Site Hostname	Hostname of WebEx site used by the customer. Provided by the Cisco WebEx Account Team. Example: <a href="https://example.webex.com">example.webex.com</a> See <a href="#">Configure Cisco TelePresence Management Suite</a> , on page 107 for instructions.	

What You Need	Description and Source	Done
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>Provided by the Cisco WebEx Account Team.</p> <p>Example: https://example.webex.com/admin</p> <p>See <a href="#">Integrate Cisco TelePresence with a Cisco WebEx Site Administration Account</a>, on page 151 for instructions.</p>	
Cisco WebEx Administrator username	<p>Cisco WebEx Site Administrator account username.</p> <p>Provided by the Cisco WebEx Account Team.</p> <p>Example: webexAdmin</p> <p>See <a href="#">Integrate Cisco TelePresence with a Cisco WebEx Site Administration Account</a>, on page 151 for instructions.</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>See <a href="#">Configuring Single Sign On in Cisco TMS</a>, on page 118 for instructions.</p>	

What You Need	Description and Source	Done
Client/server certificate for Cisco VCS Expressway	<p>Because the call leg between the Cisco VCS Expressway and the WebEx cloud must be encrypted, .</p> <p>See <a href="#">Cisco Expressway and TelePresence Configuration Tasks, on page 82</a> and <a href="#">Configure Certificates on Cisco Expressway-E and Cisco VCS Expressway, on page 95</a> for instructions.</p>	







## Deployment Options

---

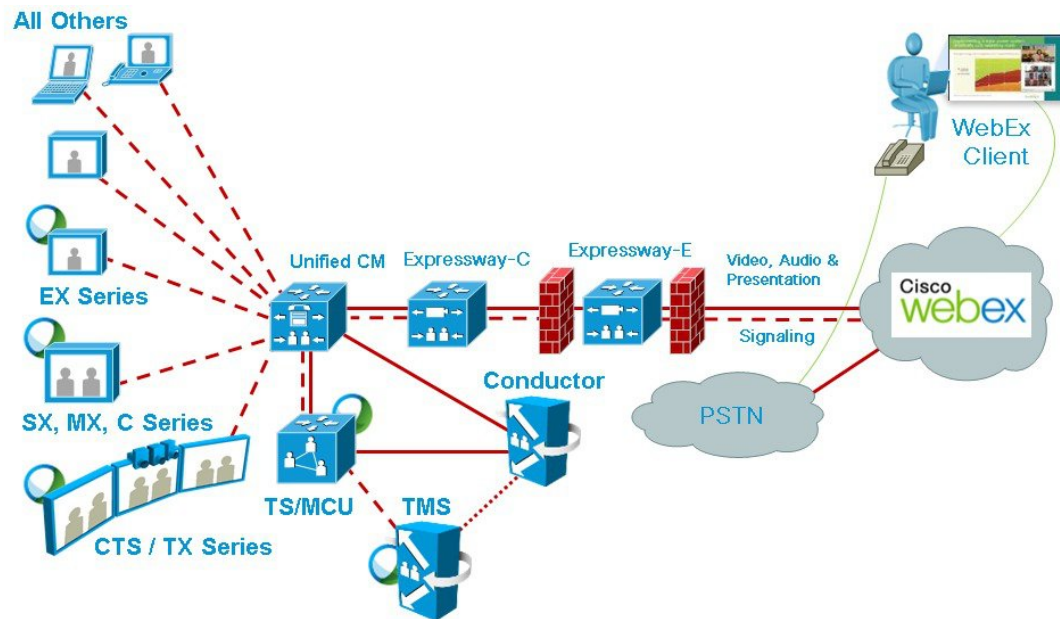
- [SIP Video, Presentation, and Audio in a Unified CM-centric Deployment, page 29](#)
- [SIP Video, Presentation, and PSTN Audio in a Unified CM-centric Deployment, page 30](#)
- [SIP Video, Presentation, and Audio in a VCS-centric Deployment, page 32](#)
- [SIP Video, Presentation, and PSTN Audio in a VCS-centric Deployment, page 32](#)

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

WebEx is deployed using WebEx Audio. Main video, content, and audio to and from the WebEx cloud is negotiated between the Cisco Expressway-E on the customer site and the WebEx Cloud. All media (main

video, content, and audio) flows over IP negotiated using SIP. Blue and green balls symbolize WebEx-enabled endpoints (ball displayed on endpoint display) (OBTP).

**Figure 1: Network Topology - SIP Video, Audio and Presentation**



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

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

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

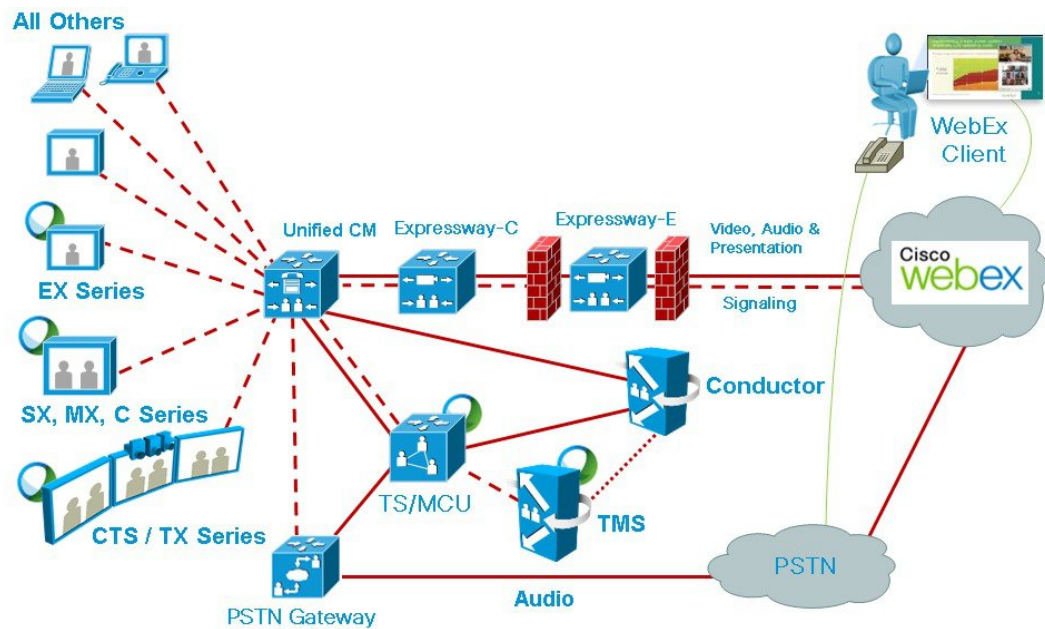
This deployment can be set up either of the following ways:

- Using a PSTN gateway registered to Unified Communications Manager.
- Using a PSTN gateway registered to Cisco Expressway-C

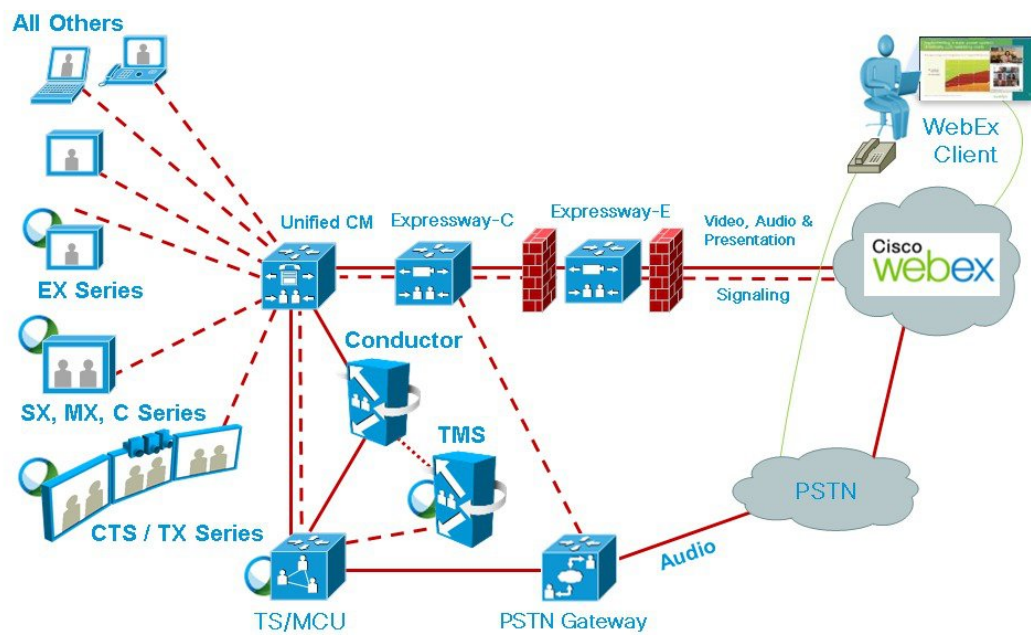
**Note**

Customers using a Codian ISDN Gateway must register it to Cisco VCS Control and therefore must use Cisco VCS.

**Figure 2: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified Communications Manager**



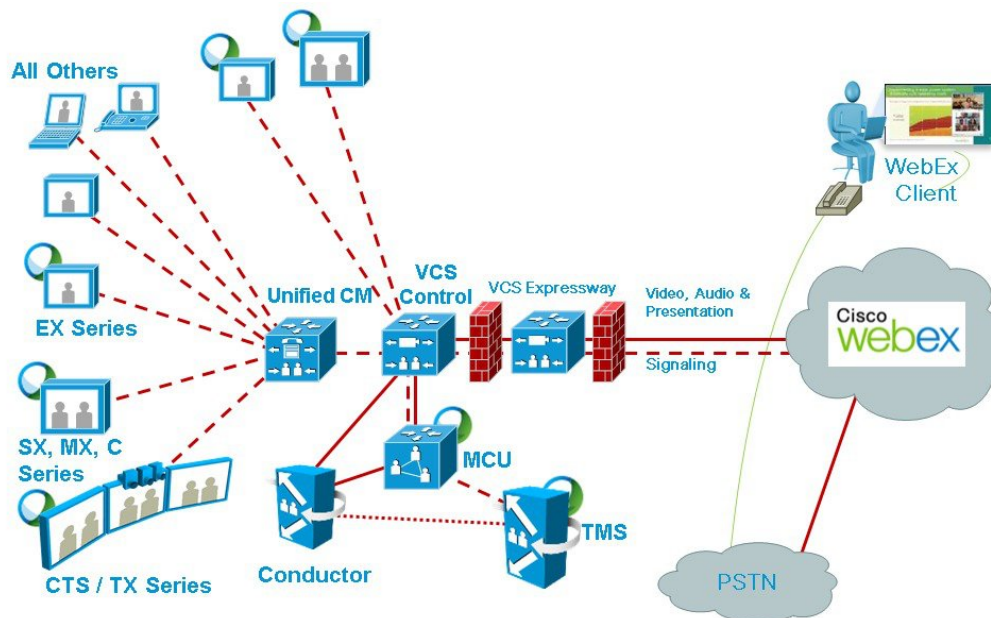
**Figure 3: Network Topology - SIP Video and Presentation with PSTN Audio Using Cisco Expressway-C**



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

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

**Figure 4: Network Topology - SIP Video, Audio and Presentation**



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

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

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

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

- Using a PSTN gateway registered to Unified Communications Manager.

- Figure 5: Network Topology - SIP Video and Presentation with PSTN Audio Using Unified Communications Manager**









## Requirements

---

- [CMR Hybrid Prerequisites, page 36](#)
- [Conference Bridges, page 42](#)
- [Multiparty Licensing, page 42](#)
- [TelePresence Conductor, page 43](#)
- [Default SIP TCP Timeout in Cisco Expressway / Cisco VCS, page 43](#)
- [Security and Encryption, page 43](#)
- [Resilience and Clustering, page 44](#)
- [SIP Early Offer Messaging, page 45](#)
- [Bridge Pools and Service Preferences, page 45](#)
- [Content Channel, page 46](#)
- [H.323 Interworking, page 46](#)
- [Microsoft Lync 2013 Interoperability, page 46](#)
- [Recommended Screen Resolutions for Presentation Sharing, page 46](#)
- [Network and Client Restrictions that Affect Video in the WebEx Client, page 47](#)

# CMR Hybrid Prerequisites

## CMR Hybrid Product and Service Requirements

**Table 11: CMR Hybrid Product and Service Requirements**

Requirement	Description	Minimum Version	Recommended Version
Cisco TelePresence Conductor	<p>TelePresence Conductor is required for conference resource allocation and management of conference bridges.</p> <p>Required for use with certain TelePresence Servers and MCUs. Refer to the documentation for the bridges you plan to use to determine if Conductor is required.</p> <p>The TelePresence Conductor must be deployed using its back-to-back user agent (B2BUA). The external policy server interface is not supported.</p>	<p>XC3.0</p> <p>XC3.0.2 is required for TSP audio</p>	XC4.0 or later
Cisco TelePresence Management Suite (Cisco TMS)	Cisco TMS is required for scheduling CMR Cloud meetings.	14.6	<p>15.0 or later</p> <p>Required with TMSXE 5.0, and WebEx Meeting Center WBS30 or later to get the new WebEx Productivity Tools features. For more information, refer to the <a href="#">release notes</a>.</p>
Microsoft SQL Server	Database for Cisco TMS.	2008 R2 64-bit	2012 SP2 64-bit



Requirement	Description	Minimum Version	Recommended Version
Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE)	Cisco TMSXE is required for scheduling CMR Hybrid meetings through Microsoft Outlook using either the WebEx Productivity Tools Plug-in or WebEx Scheduling Mailbox Scheduling.	4.1.	5.0 or later  Required with TMS 15.0 and WebEx Meeting Center WBS30 or later to get the new WebEx Productivity Tools features. For more information, refer to the <a href="#">release notes</a> .
Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE)	Cisco TMSPE is required for scheduling Cisco Collaboration Meeting Rooms (CMR) Hybrid meetings using Smart Scheduler.  <b>Note</b> Use of Smart Scheduler does not require the TMS provisioning option key.	1.4	1.5 or later
Cisco Expressway	Cisco Expressway-C and Cisco Expressway-E are required for Unified CM-centric deployments.  <b>Note</b> Note: A Unified CM license is required to purchase Cisco Expressway.	X8.5.3	X8.6.1 or later (for free traversal/RMS calls to WebEx with full URI dialing)
Cisco Unified Communications Manager (Unified Communications Manager)	Unified Communications Manager is required for Unified CM-centric deployments and can also be used with VCS-centric deployments if endpoints are registered to Unified Communications Manager.	10.5(2) SU1	10.5(2) SU2 or later
Cisco TelePresence Video Communication Server	(Optional) To support calls from legacy/H.323 endpoints in your network, they must be registered to Cisco VCS.	X8.5.3	X8.6.1 or later (for free traversal/RMS calls to WebEx with full URI dialing)

Requirement	Description	Minimum Version	Recommended Version
Cisco TelePresence Server	TelePresence Server can be used as a conference bridge for CMR Hybrid meetings.  TelePresence Server bridges are trunked to the TelePresence Conductor and must be configured for remote management by the TelePresence Conductor.	4.1	4.2 or later
Cisco TelePresence MCU Series	Cisco TelePresence MCU Series can be used as a conference bridge for CMR Hybrid meetings.	4.4	4.5 or later  Required for Unified Communications Manager-centric deployments.

Requirement	Description	Minimum Version	Recommended Version
Cisco WebEx Meeting Center	The WebEx Meeting Center site must be configured to support Cisco TelePresence Integration. See <a href="#">Integrate Cisco TelePresence with a Cisco WebEx Site Administration Account, on page 151</a> for more information.	WBS29.11 with the latest service pack.	WBS30 or later with the latest service pack.  Required with TMS 15.0 and TMSXE 5.0 or later to get the new WebEx Productivity Tools features. For more information, refer to the <a href="#">release notes</a> .
	<b>Resource Allocation Guidelines (per Meeting)</b> - Bandwidth must be at least 1.3 mb/sec per WebEx Meeting Center client for the best possible experience. - Where WebEx clients connect via TCP they will be less tolerant of network impairments and more likely to request a downspeed from WebEx vs UDP. Open UDP ports 9000/9001 to WebEx Meeting Center clients.		
	<b>Account Validation Guidelines</b> Each user who is scheduling Cisco Collaboration Meeting Rooms (CMR) Hybrid meetings in Cisco TMS, must have a host account on the WebEx site. 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. Cisco TMS validates authorized Cisco WebEx account holders. <b>Note</b> WebEx password is not required if Single-Sign-On (SSO) is configured in TMS. See <a href="#">Configuring Single Sign On in Cisco TMS, on page 118</a> for more information.		
Supported Endpoints	Any endpoint supported by TelePresence Server or MCU can join a CMR Cloud meeting.  In order to present to WebEx participants, the endpoint must support the BFCP protocol.	N/A	

## CMR Hybrid CPU Requirements

*Table 12: CMR Hybrid CPU Requirements*

Requirement	Description
CPU power—Recommendation for good video quality and integrating the Cisco TelePresence network with Cisco WebEx.	Suggested CPU power (depends on running applications) is dual core CPU, 2.5 GHz memory running at least 2G.

## CMR Hybrid Network Requirements

*Table 13: CMR Hybrid Network Requirements*

Requirement	Description
Network Requirements and Recommendations	<p>To ensure best results with CMR Hybrid, customer should comply with the following network requirements and recommendations:</p> <ul style="list-style-type: none"> <li>• UDP connection from customer premises to WebEx with no more than 6-8% packet loss. Make sure UDP is selected in the WebEx Site Administration settings. For details, refer to <a href="#">Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account</a>, on page 151</li> <li>• Network connection from customer premises to WebEx over the public Internet must not exceed 1% packet loss. To achieve satisfactory video quality, packet loss should be below 0.05%.</li> <li>• Network bandwidth should be at least 2-4 Mbps upstream between the MCU/TelePresence Server and Cisco WebEx. For example, if you are anticipating 5 simultaneous Cisco WebEx calls, you will need to have five 2-4 Mbps bandwidth instances.</li> </ul>

## IP Ranges, Protocols and Ports Used by CMR Hybrid

To ensure best results with CMR Hybrid, Cisco recommends customers to allow connectivity to all of the following IP ranges and ports:

**IP Ranges**

## US/Canada

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

## APAC

- 210.4.192.0/20 (CIDR) or 210.4.192.0 - 210.4.207.255 (net range)
- 114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range)

## EMEA

- 62.109.192.0/18 (CIDR) or 62.109.192.0 - 62.109.255.255 (net range)

**Table 14: Protocols and Ports Used by WebEx Client for Inbound and Outbound Communication (Windows and Mac)**

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

**Table 15: Ports Used by Expressway-Edge or VCS-Expressway for Outbound Calls from TelePresence Endpoints**

Protocol	Port Number	Access Type
----------	-------------	-------------

TCP	5060 - 5065	Call Signaling (Primary and Backup)
UDP	36000 - 59999	Call Media (Primary and Backup)

**Note**

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

As a result, it is highly recommended to disable SIP and H.323 application layer gateways on routers/firewalls carrying network traffic to or from a VCS Expressway or Expressway-E, because, when these are enabled they can negatively affect the built-in firewall/NAT traversal functionality of the VCS

## Conference Bridges

The primary deployment architecture for the solution uses TelePresence Server conference bridges. (In this release we also support MCUs as an optional addition.) The conference bridges are trunked to the TelePresence Conductor.

- TelePresence Servers must be configured for remote management by Conductor, in the case of models where this is a configurable option.
- To support Multiparty Licensing, connections between TelePresence Conductor and the conference bridges must use HTTPS.
- H.323 must be disabled on the conference bridges.

## Multiparty Licensing

Multiparty Licensing lets you administer licenses centrally on the Cisco TelePresence Conductor instead of loading screen licenses locally onto the Cisco TelePresence Servers. Two variants are available:

- Personal Multiparty (PMP) licenses, which apply to named individual hosts.

PMP licenses are purchased through Cisco Unified Workspace Licensing (CUWL Pro). They are available for deployments with Unified CM for call control.

- Shared Multiparty (SMP) licenses, which are shared between hosts and apply for the duration of the conference.

SMP licenses are available for deployments with either Unified CM or Cisco VCS for call control.

Each TelePresence Conductor can support either Multiparty Licensing or TelePresence Server screen licensing, but not both together. If you have a mix of TelePresence Server and Cisco TelePresence MCU Series conference bridges however, you can use Multiparty Licensing for the TelePresence Servers and port licensing for the MCUs together on the same Conductor.

## TelePresence Conductor

The TelePresence Conductor must be deployed using its back-to-back user agent (B2BUA). The external policy server interface is not supported.

If you use Multiparty Licensing, you do not need screen licenses on the TelePresence Servers. Instead the Multiparty Licenses are managed centrally by TelePresence Conductor.

If you have Cisco TelePresence MCU Series bridges, although they can be added to a Conductor running in Multiparty Licensing mode, you need to install port licenses on the individual bridges.

## Default SIP TCP Timeout in Cisco Expressway / Cisco VCS

From Cisco Expressway / Cisco VCS Version X8.5.3 the SIP TCP timeout value is configurable. The default value is 10 seconds. We strongly recommend that you set the timeout to the lowest value that is appropriate for your deployment. A value of 1 second is likely to be suitable in most cases, unless your network has extreme amounts of latency (such as video over satellite communications).

If an outbound call is placed to an external DNS destination, and that destination has secondary/tertiary servers and the primary server is out of service, it will take N seconds (where N is the timeout value) to timeout and try the secondary server, and N seconds again to timeout and try the tertiary server, and so on. This applies to B2B point to point calls and calls into cloud-based hosted services.

To set the SIP TCP timeout value:

### Procedure

- 
- Step 1** Access the command line interface (this setting cannot be configured through the web interface).
- Step 2** Type the following command, replacing "n" with the required timeout value: xConfiguration SIP Advanced SipTcpConnectTimeout: n  
Example: xConfiguration SIP Advanced SipTcpConnectTimeout: 1
- 

## Security and Encryption

### Signaling traffic

TLS encryption is mandatory for TelePresence Conductor-to-bridge SIP communication, and Multiparty Licensing requires HTTPS connections between Conductor and the bridges. We also recommend TLS for all other SIP (and XML RPC) communication in the solution—between endpoints and the call controller, and between the call controller and TelePresence Conductor.

### Media traffic

SRTP encryption is recommended for media traffic. For a call to support SRTP encrypted media, its associated SIP signaling must use TLS for all hops, as follows:

- 1 Between the endpoint and the call controller.
- 2 Between the call controller and TelePresence Conductor.

- 3 Between TelePresence Conductor and the conference bridge (always mandatory anyway).

**Caution**


---

Unless TLS signaling is in place for all three elements, the call cannot support SRTP.

---

## Configuration Summary

Conference bridges must be configured to use TCP port 5061 and signaling mode TLS (SIP Settings page). From TelePresence Server Version 4.2, HTTPS and SIP signaling over TLS does not need an encryption key installed on the conference bridges. For media encryption, you still need to install a media encryption key. Port 443 is the default for HTTPS; port 5061 is the default for TLS.

Specify TCP port 5061 and TLS signaling mode on the TelePresence Conductor **Location** and on the call controller (**SIP Trunk Security Profile**). See [Cisco TelePresence Conductor with Unified Communications Manager Deployment Guide](#) for details.

### Media encryption from Cisco Expressway / Cisco VCS

If you want to apply media encryption to calls that egress the Expressway solution towards DNS Zone destinations, we strongly recommend that you use this approach:

#### Procedure

- 
- Step 1** Enable media encryption on the traversal client zone, from the Cisco Expressway-C / Cisco VCS Control towards the Cisco Expressway-E / Cisco VCS Expressway. To do this set **Media encryption mode** to **Best effort** or **Force encrypted**, depending on your security policy.
  - Step 2** Disable additional, unnecessary media encryption on the DNS egress zone, from the Cisco Expressway-E / Cisco VCS Expressway towards the Internet. To do this set **Media encryption mode** on that zone to **Auto**.
- 

## Resilience and Clustering

We recommend that the solution components are deployed in cluster configurations, to provide redundancy in case of a failure. Deploying clusters of TelePresence Conductors and multiple bridge pools ensures resilience for escalated and Personal CMR / rendezvous conferences.

Resiliency is not supported for conferences scheduled via Cisco TMS. Although Cisco TMS supports multiple TelePresence Conductors, this is for scale and not for resilience. If the TelePresence Conductor configured in Cisco TMS is down, the administrator needs to manually fail over to another TelePresence Conductor cluster member in TMS.

For details about Conductor clustering see [Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide](#).



# SIP Early Offer Messaging

Early Offer messaging is strongly recommended for all Unified CM-connected SIP trunks that carry TelePresence calls, and is required for CMR Hybrid conferences and some third-party services. Cisco VCS-Centric deployments always run in Early Offer mode, except for H.323 to SIP interworked calls. (Because H.323 uses Slow Start signaling mode on Cisco VCS and Cisco Expressway, SIP messaging for interworked calls is done using Delayed Offer.)

## Bridge Pools and Service Preferences

- At least one Service Preference is required in TelePresence Conductor. You can optionally place all conference bridge pools into a single Service Preference.
- All conference bridges must be assigned to a conference bridge pool in TelePresence Conductor. Each conference bridge can belong to only one pool.
- All conference bridges in a TelePresence Conductor pool must be of the same type (MCU or TelePresence Server). Usually it is best to configure a pool with bridges from the same location, although this is optional, not mandatory.
- As with pools, all conference bridges in a Service Preference must be of the same type (MCU or TelePresence Server).
- All conference bridges within a pool must be configured identically.
- We strongly recommend that all conference bridges within a pool have the same capacity, so that conferences can be distributed efficiently across conference bridges. If conference bridges with different capacities exist in the same pool, unbalanced conference placement may occur in some scenarios.
- If Unified CM call admission control is implemented to control bandwidth usage, each Service Preference must only contain pools of bridges for a single location.
- For scheduled conferences, two configuration methods for pools and Service Preferences are possible:

Our recommended approach is to allow the TelePresence Conductor to manage resources that are shared across all conference types, including scheduling. This gives the best trade off between utilization of resources, user experience, and availability. When peak hour usage increases, you should consider adding more bridges. You can use the Capacity Adjustment setting in Cisco TMS to control over- or undersubscription (see Task 8: Edit Service Preferences in Cisco TMS (optional), page 39).

- Or, to avoid the situation where scheduled conferences may be impacted because resources have already been used up by unscheduled conferences, you can dedicate a conference bridge for use only by scheduled conferences. Use a single bridge per Service Preference and configure it for scheduling in Cisco TMS.

See [Configurations for Scheduled Conferencing](#), on page 64 more details.

- We strongly recommend that all conference bridges within a pool have the same capacity, so that conferences can be distributed efficiently across conference bridges. If conference bridges with different capacities exist in the same pool, unbalanced conference placement may occur in some scenarios.
- Make sure that aliases dialed from endpoints connected to Unified CM only use bridges in the Location expected by Unified CM. If bridges in a different Location are specified and used, Unified CM accounts

for the call bandwidth in the wrong Location. Bandwidth will be wrongly allocated to the expected Location, with no bandwidth allocated to the actual Location.

## Content Channel

Most TelePresence endpoints support the use of a second video channel known as the content channel. Typically this is used for presentations running alongside live video.

- For MCU conference bridges, set the **Content mode** for the Conference template in TelePresence Conductor to Transcoded (**Advanced parameters**). When this mode is selected in a TelePresence Conductor template, a dedicated content port or video port will be allocated depending on the MCU model and configuration.
- For TelePresence Server conference bridges, currently the content mode is always Transcoded and is not configurable.

## H.323 Interworking

The CMR Hybrid network is SIP-based. To connect H.323 endpoints to conferences within the CMR Hybrid network, the call must be interworked before reaching the TelePresence Conductor. To do this configure the Cisco VCS Control or Cisco Expressway-C to perform the necessary SIP/H.323 interworking.

- To interwork only for locally registered endpoints, set the **H.323 <-> SIP interworking mode to Registered only** (accessed from VCS configuration > Protocols > Interworking).
- To optionally allow interworking of business-to-business H.323 calling between external networks and your conferences, set the **H.323 <-> SIP interworking modes** to On. This will interwork all incoming calls.

## Microsoft Lync 2013 Interoperability

CMR Hybrid supports interoperability with the Microsoft Lync 2013 service via interworking by the Cisco Expressway-C (needs the Microsoft Interoperability key). For capacity reasons we recommend that you implement separate Cisco Expressway-C devices for Lync access, and for other networking requirements respectively.

## 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

# Network and Client Restrictions that Affect Video in the WebEx Client

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

**Note**

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





## Set Up the Solution Components

- [Set Up the Conference Bridges, TelePresence Conductor, and Unified Communications Manager](#), page 49
- [Enable Personal CMRs](#), page 50
- [Manage Multiparty Licensing](#), page 55

## Set Up the Conference Bridges, TelePresence Conductor, and Unified Communications Manager

### Before You Begin

- Cisco TelePresence Conductor must be installed according to the instructions in [Cisco TelePresence Conductor Getting Started](#) or [Cisco TelePresence Conductor Virtual Machine Installation Guide](#).
- Cisco Unified Communications Manager must be installed and configured with a base configuration. Ensure connectivity by registering at least three endpoints, and make sure they are all capable of calling each other with voice and video communications.
- One or more conference bridges must be powered on and accessible to the Cisco TelePresence Conductor over HTTP/HTTPS and SIP TLS. HTTPS is recommended in all cases and is required for Multiparty Licensing to work.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p>Complete the following tasks in <a href="#">Cisco TelePresence Conductor with Unified CM Deployment Guide (XC4.0)</a>:</p> <ul style="list-style-type: none"><li>• Configuring the Cisco TelePresence MCU Series (if applicable).</li><li>• Configuring the TelePresence Server.</li></ul>	In CMR Hybrid, the TelePresence Conductor is deployed using its B2BUA. The external policy service interface is not supported.

	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>Configuring the TelePresence Conductor's general settings.</li> <li>Configuring the Unified CM's general settings.</li> </ul>	
<b>Step 2</b>	<a href="#">Enable Personal CMRs, on page 50</a>	Optional. If you want to use PMP licenses with scheduled conferences, you must enable Personal CMRs for each license group. When Cisco TMS creates a scheduled conference, TelePresence Conductor looks through the list of Personal CMRs. If there is a Personal CMR with a PMP license defined for the user, the PMP license is used. If there is no matching user, an SMP license is used.
<b>Step 3</b>	<a href="#">Manage Multiparty Licensing , on page 55</a>	We recommend that you enable Multiparty Licensing. Use these procedures if you have TelePresence Server conference bridges and use Multiparty Licensing. In this case, you administer licenses centrally on the Cisco TelePresence Conductor instead of loading screen licenses onto the bridges.
<b>Step 4</b>	Enable scheduled conferencing. Refer to <a href="#">Enable Scheduling in TelePresence Conductor and Cisco TMS, on page 67</a> for details.	

## Enable Personal CMRs

The primary function of Personal Collaboration Meeting Rooms (CMRs) is to provide virtual rooms for users to host meetings and collaborate with others. Using Cisco TMSPE, administrators provision Personal CMRs on TelePresence Conductor for groups of users. Users can then activate and personalize their own CMR through a user portal.

## Role of Personal CMRs in Multiparty Licensing

If you use Multiparty Licensing, then Personal CMRs have a secondary function. For deployments with a mix of Personal Multiparty (PMP) and Shared Multiparty (SMP) licenses they provide a mechanism for administrators to define whether each user in a particular user group should be allocated a PMP or an SMP license. This mechanism is used for all conference types, including scheduled conferences.

- If a user does not have a Personal CMR, they consume SMP licenses for any scheduled conferences they initiate.

- If a user has a Personal CMR, they consume a PMP license if the **Multiparty Licensing Mode** value for the CMR template is left to the default (**Personal Multiparty**). Their PMP license is used for any scheduled or CMR conferences they initiate.
- If a user has a Personal CMR, and the **Multiparty Licensing Mode** value is changed to Shared Multiparty, they consume SMP licenses for their conferences.

If you don't want a user to consume SMP licenses for their conferences and the user does not already have a Personal CMR, you need to provision a Personal CMR with the default licensing mode (**Personal Multiparty**). If the user has a Personal CMR, then no action is needed unless you previously changed the default licensing mode.

Summary	
Does user have a Personal CMR?	Then user consumes this license type...
No	SMP
Yes - PMP mode	PMP
Yes - SMP mode	SMP

For details about administrator tasks for Multiparty Licenses, see [Manage Multiparty Licensing](#) , on page 55.

## Personal CMR Templates and Conductor Conference Templates

The CMR template corresponds to a conference template and a conference alias on TelePresence Conductor. CMRs created by using Cisco TMSPE cannot be modified through the TelePresence Conductor web user interface. Conference templates and aliases created by using TelePresence Conductor cannot be modified through Cisco TMSPE.

## Enable Personal CMRs Task Flow

### Before You Begin

- The TelePresence Conductor must have at least one populated bridge pool and Service Preference.
- Cisco TMSPE must be installed and enabled in Cisco TMS.
- Cisco TMSPE is accessed from the **Systems > Provisioning** menu in Cisco TMS.
- A user base must exist for Cisco TMSPE. For information on how to set up a user base see section *Creating groups and adding users* in [Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide](#).

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Create a TelePresence Conductor User with API Access, on page 52</a>	Create an API-enabled user account for Personal CMRs on each TelePresence Conductor or cluster.
<b>Step 2</b>	<a href="#">Add the TelePresence Conductor API User to Cisco TMSPE, on page 53</a>	
<b>Step 3</b>	<a href="#">Enable WebEx for Personal CMRs, on page 53</a>	Optional.
<b>Step 4</b>	<a href="#">Create CMR Templates, on page 54</a>	Create one or more CMR templates to specify the base dial plan for CMR URIs and numeric aliases.
<b>Step 5</b>	<a href="#">Apply CMR Templates to Groups, on page 54</a>	Apply the templates to Active Directory user groups.
<b>Step 6</b>	<a href="#">Enable Monitoring for Personal CMRs, on page 54</a>	Optional. If you want to enable monitoring, add the TelePresence Conductor to Cisco TMS. You must do this even though TelePresence Conductor has been added to Cisco TMSPE.
<b>Step 7</b>	<a href="#">Synchronize CMRs, on page 54</a>	Active Directory users are regularly synchronized with Cisco TMS. After synchronizing, TMS emails the CMR details to the affected users so they can activate their CMRs.
<b>Step 8</b>	Users activate their CMRs.	The CMR is created on TelePresence Conductor when the user activates it. When a Personal CMR is created, Cisco TMSPE applies the settings in the CMR template associated with the user's group, creates the room on TelePresence Conductor, and emails the user. No further interaction is needed from you as the administrator.

**What to Do Next**

You can now use the following conference methods:

- Scheduled conferences using PMP or SMP licenses
- Personal CMRs

**Create a TelePresence Conductor User with API Access****Procedure**

In TelePresence Conductor, go to **Users > Administrator** accounts and create a User with the following attributes:



- **Access level:** Read-write
- **Web access:** No
- **API access:** Yes
- **State:** Enabled

## Add the TelePresence Conductor API User to Cisco TMSPE

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users**.
- Step 2** Click **TelePresence Conductor Settings**.
- Step 3** Click **Add New**.
- Step 4** In the TelePresence Conductor Configuration dialog, add the TelePresence Conductor details and user credentials: Hostname/IP: Hostname or IP address of the TelePresence Conductor.
- **Port:** Port to connect on (default is HTTPS on port 443)
  - **Username / Password:** The credentials for the Conductor user that you created in the previous step.
  - **Domain:** TelePresence Conductor will append this domain for all numeric aliases created through Cisco TMSPE.
  - Click **Save**.
- 

## Enable WebEx for Personal CMRs

If you already have CMR Hybrid deployed, you can optionally enable it in Personal CMRs to allow joint participation by Cisco WebEx and TelePresence users. If this is a first-time CMR Hybrid deployment, you can do this as a separate task later, as described in *Using CMR Hybrid with Personal CMRs*, and regenerate the CMRs at that point. Or you can do it now, before you define the CMRs.

### Procedure

- 
- Step 1** In Cisco TMS, go to **Administrative Tools > Configuration > Provisioning Extension Settings**.
- Step 2** Under **Collaboration Meeting Room**, set **Allow WebEx Connections** to **Yes**.
- Step 3** Click **Save**.
- If you do it now, remember to check Include WebEx when you create the CMR templates in the next step.
-

## Create CMR Templates

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users**(to access Cisco TMSPE).
- Step 2** Under **Collaboration Meeting Room Templates**, create one ore more templates as required
- If this CMR template is for users with a PMP license, set **Multiparty License Mode** to *Personal Multiparty* on the CMR Template.
  - The **SIP Alias Pattern** specifies the URI pattern that users can dial to connect into the CMR. The **Numeric Alias Pattern** optionally specifies numeric dialing in addition, which can be based on number ranges or on regex patterns (*Office Phone* or *Mobile Phone* in Active Directory).
  - Check **Include WebEx** if you have CMR Hybrid and want to allow WebEx users to access the room.
- 

## Apply CMR Templates to Groups

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users**.
- Step 2** Choose the relevant group, then select the button for the required template in the **Active** column.
- 

## Enable Monitoring for Personal CMRs

Optional. If you want to enable monitoring, you must complete this procedure even though TelePresence Conductor has been added to Cisco TMSPE.

### Procedure

Add the TelePresence Conductor to Cisco TMS. See the Cisco TMS context-sensitive help or the Cisco TelePresence Management Suite Administrator Guide at <http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html>. Search for "Adding systems".

## Synchronize CMRs

Cisco TMSPE automatically synchronizes all Personal CMRs once per day. You can either wait for the synchronization to occur or (if you want to use the Personal CMRs or PMP licenses straight away) you can manually synchronize the CMRs.

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users**.
- Step 2** Under **Collaboration Meeting Room Templates**, click on **TelePresence Conductor Settings**.
- Step 3** In the dialog window that opens, find the relevant TelePresence Conductor and click the icon for it. The icon is on the right-hand side (with a tool-tip labeled **TelePresence Conductor Multiparty Licensing**).
- Step 4** In the dialog window that opens, click **Synchronize Now**.  
When the synchronization completes, Cisco TMS notifies the affected users by email that their Personal CMRs are available. Users can now activate and customize their CMRs through the Cisco TMSPE User Portal. When a user activates their CMR, it is created on TelePresence Conductor.
- 

## Manage Multiparty Licensing

Use the procedures in this section if you have TelePresence Server conference bridges and use Multiparty Licensing. In this case, you administer licenses centrally on the Cisco TelePresence Conductor instead of loading screen licenses onto the bridges.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Enable Multiparty Licensing, on page 55</a>	We recommend that you enable Multiparty Licensing.
<b>Step 2</b>	<a href="#">Apply Licenses to Users, on page 56</a>	If you have a mix of Shared Multiparty (SMP) and Personal Multiparty (PMP) licenses, you can define whether each user in a particular user group should be allocated a PMP or an SMP license. Use this procedure to check what license type is in use for a given user group.
<b>Step 3</b>	<a href="#">Change the Licensing Mode, on page 56</a>	Use this procedure to change the licensing mode for a given user group.
<b>Step 4</b>	<a href="#">Manually Synchronize Licenses, on page 57</a>	Use this procedure if you want to use PMP licenses straight away without waiting for the automatic synch to occur.
<b>Step 5</b>	<a href="#">Monitor License Use, on page 57</a>	Use this procedure to view how many licenses are installed, how many PMP licenses are assigned to users, and the peak usage of SMP licenses in the last 60 days.

## Enable Multiparty Licensing

We recommend that you enable Multiparty Licensing.

### Procedure

- 
- Step 1** Log in to your TelePresence Conductor.
  - Step 2** Ensure there are no active calls on your TelePresence Conductor. Any currently active calls are ended when you enable Multiparty Licensing.
  - Step 3** Go to **Maintenance > Option keys**.
  - Step 4** Under **Software option** in the **Add option key** field, enter the option key for the Personal Multiparty (PMP) or Shared Multiparty (SMP) licenses you have purchased.
  - Step 5** Click **Add option**.
  - Step 6** Repeat for any other PMP and SMP license keys you have purchased. License keys are additive, so for example, two option keys for 100 Personal Multiparty licenses result in 200 Personal Multiparty licenses.
  - Step 7** On the same page, under **Multiparty Licensing**, set **Multiparty licensing for TelePresence Servers** to Enabled.
- 

## Apply Licenses to Users

If you have a mix of Shared Multiparty (SMP) and Personal Multiparty (PMP) licenses, you can define whether each user in a particular user group should be allocated a PMP or an SMP license. Users consume a Shared Multiparty (SMP) license for their conferences, unless they have a Personal CMR provisioned and the Personal CMR specifies Personal Multiparty (PMP) licensing mode (the default). You should do this when you set up the Personal CMRs. See [Enable Personal CMRs, on page 50](#).

To check what license type is in use for a given user group:

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users > Collaboration Meeting Rooms Templates**.
  - Step 2** Select the template concerned.
  - Step 3** The **Multiparty License Mode** drop-down determines what licensing mode is applied for the users groups with this template assigned.
- 

## Change the Licensing Mode



### Caution

This process relates to changing the licensing mode. Other changes to templates are potentially disruptive and need pre-planning. For more information, refer to 'Managing Administration Changes to personal CMRs in the following guide: <http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/solutions/cmrpremises/cmr-premises-deployment-guide-r5-0.pdf>.

To change the licensing mode for a given user group:

### Procedure

- 
- Step 1** Ensure that sufficient PMP or SMP licenses (as appropriate) are available to support the change.
  - Step 2** In Cisco TMS, go to **Systems > Provisioning > Users > Collaboration Meeting Room Templates**.
  - Step 3** Select the template concerned.
  - Step 4** Set the **Multiparty License Mode** drop-down as required. To apply PMP licenses to users, select **Personal Multiparty**.
  - Step 5** Click **Save**.
  - Step 6** The counter next to **Check sync status** indicates how many CMRs are out of sync with the modified template. Click **Regenerate CMRs** to synchronize the change on TelePresence Conductor.
- 

## Manually Synchronize Licenses

Personal Multiparty (PMP) licenses are automatically synchronized by Cisco TMSPE's daily synch of the associated Personal CMRs. If you want to use PMP licenses straight away without waiting for the automatic synch, you can synchronize manually:

### Before You Begin

We recommend that you synchronize during a maintenance window, or at least avoid doing it in peak hours.

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users**.
  - Step 2** Under **Collaboration Meeting Room Templates**, click on **TelePresence Conductor Settings**.
  - Step 3** Find the relevant TelePresence Conductor and click on its icon. The icon is on the right-hand side (with a tool-tip labeled 'TelePresence Conductor Multiparty Licensing').
  - Step 4** Click **Synchronize Now**.
- 

## Monitor License Use

You can view how many licenses are installed, how many PMP licenses are assigned to users, and the peak usage of SMP licenses in the last 60 days:

### Procedure

In TelePresence Conductor go to **Status > Multiparty licenses**.





## CHAPTER

# 6

## Connect Cisco TelePresence Conductor to Call Control

---

- [Connect TelePresence Conductor to Cisco Unified Communications Manager, page 59](#)
- [Connect TelePresence Conductor to Cisco VCS, page 60](#)

## Connect TelePresence Conductor to Cisco Unified Communications Manager

This procedure provides an overview of the steps that you must complete to configure the TelePresence Conductor for CMR Hybrid in Unified Communications Manager-Centric deployments. For detailed instructions, see the [Cisco TelePresence Conductor with Unified CM Deployment Guide \(XC3.0\)](#).



### Note

In CMR Hybrid, the TelePresence Conductor is deployed using its B2BUA. The external policy service interface is not supported.

### Before You Begin

- Cisco TelePresence Conductor must be installed according to the instructions in [Cisco TelePresence Conductor Virtual Machine Installation Guide](#).
- Cisco Unified Communications Manager must be installed and configured with a base configuration. Ensure connectivity by registering at least three endpoints, and make sure they are all capable of calling each other with voice and video communications.
- One or more conference bridges must be powered on and accessible to the Cisco TelePresence Conductor over HTTP/HTTPS and SIP TLS. HTTPS is recommended in all cases and is required for Multiparty Licensing to work.

### Procedure

Use the TelePresence management interface to complete the following tasks:

- Configuring the Cisco TelePresence MCU Series.
- Configuring the TelePresence Server.
- Configuring the TelePresence Conductor's general settings and configuring it for ad hoc and rendezvous conferences.
- Configuring the Unified CM's general settings and configuring it for ad hoc and rendezvous conferences.

## Connect TelePresence Conductor to Cisco VCS

This procedure provides an overview of the steps that you must complete to configure the TelePresence Conductor for CMR Hybrid in Cisco VCS-Centric deployments. For detailed instructions, see the [Cisco TelePresence Conductor with Cisco VCS \(B2BUA\) Deployment Guide \(XC3.0\)](#).

### Before You Begin

- Cisco TelePresence Conductor must be installed according to the instructions in [Cisco TelePresence Conductor Getting Started](#) or [Cisco TelePresence Conductor Virtual Machine Installation Guide](#).
- Cisco TelePresence Video Communication Server must be installed and configured to act as a SIP registrar and proxy.
- One or more conference bridges must be powered on and accessible to the Cisco TelePresence Conductor over HTTP/HTTPS and SIP TLS.
- The VCS **Zone profile** for the trunk between Cisco VCS Control and TelePresence Conductor should be set to **Custom** with **Automatically respond to SIP searches** set to **On**. For details, see Adding the TelePresence Conductor as a neighbor zone in *Cisco TelePresence Conductor with Cisco TelePresence VCS (B2BUA) Deployment Guide XC3.0*.

### Procedure

Use the TelePresence management interface to complete the following tasks:

- Designing a dial plan.
- Configuring the Cisco TelePresence MCU Series.
- Configuring the TelePresence Server.
- Configuring Cisco VCS with a neighbor zone and search rule for TelePresence Conductor.
- Configuring the TelePresence Conductor in B2BUA mode (deployments using the Cisco VCS external policy service are not supported)





## Configure Bridge Scheduling

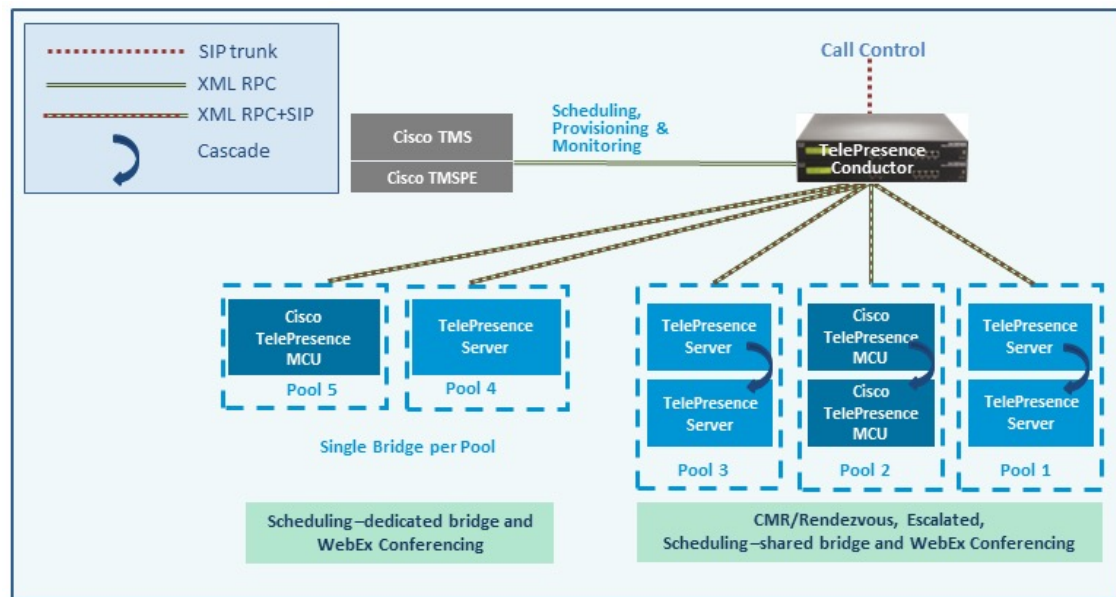
---

- [How Bridges are Scheduled in CMR Hybrid, page 61](#)
- [Limitations, page 62](#)
- [Requirements, page 63](#)
- [Configurations for Scheduled Conferencing, page 64](#)
- [Enable Scheduling in TelePresence Conductor and Cisco TMS, page 67](#)

### How Bridges are Scheduled in CMR Hybrid

Two methods for scheduling bridges are possible in CMR Hybrid:

- **Scheduling—dedicated bridge.** Deploy one or more bridges that are dedicated just for scheduled conferences, with each bridge in a pool of its own. Optionally, a second dedicated bridge and pool combination can be used as a backup.
- **Scheduling—shared bridge.** Allow bridges to be used for non-scheduled as well as scheduled conferences. In this case, resource availability for scheduled conferences cannot be guaranteed, as the necessary resources might already be in use by non-scheduled conferences.



Example configuration scenarios, and their respective advantages and disadvantages are in [Cisco Collaboration Meeting Rooms \(CMR\) Premises Solution Guide](#).

Limitations and prerequisites apply to scheduled conferencing in this release, described in:

- [Limitations](#), on page 62
- [Requirements](#), on page 63

## Limitations



### Note

If you use clustered TelePresence Conductors, be aware that Cisco TMS only recognizes one TelePresence Conductor node. If that cluster node should fail, the Cisco TMS scheduling service and its CMR provisioning service will be out of service (until the TelePresence Conductor is brought back up or Cisco TMS is updated to communicate with a different TelePresence Conductor in the cluster).

It is not possible to schedule Cisco TMSPE-provisioned CMRs.

If you use TSP Audio provided by a TSP that is configured to use the same bridge as the previous scheduled conference, we recommend that you turn off the auto-extend function in Cisco TMS.

The scheduling solution with TelePresence Conductor and Cisco TMS has some notable limitations at this time, and significant differences exist from the previous method in Release 3.0 (scheduling to direct-managed bridges). We strongly recommend before you enable scheduling, that you review the following documents:

- A table containing the differences between the previous solution method of scheduling direct-managed bridges (previous release) and scheduling TelePresence Conductor-managed bridges (this release) is available in [Cisco TelePresence Conductor with Cisco TelePresence Management Suite Deployment Guide](#).
- The Limitations section in the latest [release notes](#) for Cisco TMS.

- The Limitations section in the latest [release notes](#) for TelePresence Conductor.

## Requirements

- CMR Hybrid requires the Cisco TMS management tool for scheduling. Conferences are not scheduled directly on TelePresence Conductor.
- Ensure that the solution-level prerequisites and configuration process for CMR Hybrid are complete. In particular:
- For the Scheduling—dedicated bridge case, some additional configuration requirements apply (see below).
- Participants in a scheduled conference should not escalate to an ad hoc / instant conference. This will cause a degraded conference experience for the participants.

## Requirements for Dedicated Bridge Scheduling

If you use a dedicated conference bridge for scheduling, the following points apply:

- The bridge resources will only be used for conferencing (subject to correct configuration). In Capacity API responses to Cisco TMS, the TelePresence Conductor only returns pools that are "marked" for scheduling in the Service Preference (**Pools to use for scheduling** option).
- For additional resilience you can include one or more additional bridges / pools in the Service Preference used for scheduling. These pools should not be marked for scheduling (so they are not reported to Cisco TMS) and the additional bridges will only be used if the primary bridge becomes unavailable.
- To avoid wasting resources we recommend that you disable cascading. Even though cascading cannot physically happen, resources will still be reserved if cascading is enabled.
- Although TelePresence Server resource optimization will occur, no benefit is gained when the primary conference bridge is in use. Cisco TMS plans bridge usage ahead of actual usage, so the resources recovered by optimization are not actually re-used. If you use backup bridges which are shared resources with non-scheduled conferences, then the optimization will reduce the capacity needed on the shared backup bridge(s).

: When configuring conference bridge pools dedicated for scheduling, we recommend the following:

- Give the conference bridge pool a name indicating that it should only be used for scheduled conferences.
- Check that the pool is only used in a single Service Preference.
- Check that the Service Preference is not used in a CMR or ad hoc conference.

# Configurations for Scheduled Conferencing

Various configurations are possible to support scheduled conferencing in the solution. They are controlled by the bridge pool and Service Preference settings in TelePresence Conductor.

## Shared Bridges

Typically you might want to use this shared-bridge approach, which allows other types of conferences as well as scheduled conferences to run on the conference bridges:

**Table 16: Deploying shared bridges for scheduling**

	Service Preference contains...	Configuration	Advantages	Disadvantages
Example 1	Shared-use bridges for scheduled and non-scheduled conferences	One or more pools, shared for scheduled and nonscheduled conferences.  All pools are marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.	Cascaded conferencing available (if enabled).  Targeted management of bridge resources. Over time, monitoring of use patterns can identify the most appropriate pool configuration.	Resource availability for scheduled conferences not guaranteed (could be used up by non-scheduled conferences). This risk can be reduced by using the Capacity Adjustment setting in Cisco TMS to underallocate capacity below 100%. Only the specified reduced percentage is made available to TMS for scheduling conferences, rather than the actual capacity.

## Alternative Options (Dedicated Bridges)

If you want to reserve bridges for use just by scheduled conferences, this table provides examples of possible approaches and their advantages and disadvantages:

**Table 17: Deploying dedicated bridge(s) for scheduling**

	<b>Service Preference contains...</b>	<b>Configuration</b>	<b>Advantages</b>	<b>Disadvantages</b>
Example 2	Dedicated bridge for scheduled conferences.	<p>Single pool, with a single conference bridge.</p> <p>Pool marked to be used for scheduling in the TelePresence Conductor Service Preference. Pool is reported to Cisco TMS in capacity information requests.</p>	<p>Conference availability is guaranteed, subject to bridge failure (or full capacity).</p> <p>Maximizes use of resources, as Cisco TMS will book ports until the bridge is full.</p>	<p>Uses one conference bridge exclusively for scheduling.</p> <p>Cascaded conferencing does not occur: to avoid wasting resources, cascading should be disabled.</p>
Example 3	<ul style="list-style-type: none"> <li>• Dedicated bridge for scheduled conferences</li> <li>• Dedicated backup bridge</li> </ul>	<p>Two pools.</p> <p>Both pools contain a single conference bridge. The second pool is used as a backup if the bridge in the highest priority pool fails.</p> <p>Only the first pool is marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.</p>	<p>As for Example 2, with added benefit of fallback in case of bridge failure.</p>	<p>Uses two conference bridges exclusively for scheduling.</p> <p>Consumes backup resources.</p> <p>To avoid wasting resources, cascading should be disabled.</p>

	Service Preference contains...	Configuration	Advantages	Disadvantages
Example 4	<ul style="list-style-type: none"> <li>• Dedicated bridge for scheduled conferences</li> <li>• Shared-use backup bridges for both scheduled and non-scheduled conferences.</li> </ul>	<p>Two or more pools.</p> <p>Highest priority pool with one bridge only, used for scheduled conferences.</p> <p>Other pools contain bridges for both scheduled (as backup) and non-scheduled conferences.</p> <p>Only the first pool is marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.</p>	<p>As for Example 2, with possible benefit of fallback in case of bridge failure if the other pools have spare capacity.</p>	<p>Uses one conference bridge exclusively for scheduling.</p> <p>To avoid wasting resources on the dedicated bridge, cascading should be disabled.</p>
Example 5	<ul style="list-style-type: none"> <li>• Dedicated bridge for scheduled conferences</li> <li>• Shared-use backup bridges for both scheduled and non-scheduled conferences.</li> </ul>	<p>Two or more pools.</p> <p>Highest priority pool with two or more bridges, used for scheduled conferences. Cascading enabled on the associated conference template.</p> <p>Other pools contain bridges for both scheduled (as backup and overflow) and non-scheduled conferences.</p> <p>Only the first pool is marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.</p>	<p>As for Example 2, with possible benefit of fallback in case of bridge failure and overflow resource when cascading is used in a scheduled conference.</p> <p>Bridges in the backup pools are used for scheduling if:</p> <ul style="list-style-type: none"> <li>• A bridge in Pool 1 fails.</li> <li>• Cascading in Pool 1 uses up bridge resources that Cisco TMS expected to be available for scheduling.</li> </ul>	<p>Uses conference bridges exclusively for scheduling.</p> <p>If scheduled conferences are cascaded, they may need resources from a shared-use pool.</p>

# Enable Scheduling in TelePresence Conductor and Cisco TMS

## Before You Begin

- Ensure that the tasks in are complete in [Limitations](#), on page 62 and [Requirements](#), on page 63.
- Review the best practice guidelines for Bridge Pools and Service Preferences in [Bridge Pools and Service Preferences](#), on page 45.

## Procedure

### Step 1 Add TelePresence Conductor to Cisco TMS:

If you have not already done so, add each TelePresence Conductor that you plan to use for scheduling, as a system in Cisco TMS, and associate each system with the appropriate zone. See the Cisco TMS help or the Cisco TMS Administrator Guide (search for "Adding Systems") at the following URL on Cisco.com: <http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html>

**Note** If you use clustered TelePresence Conductors, define only one node per cluster to Cisco TMS.

### Step 2 Define IP Zone for TelePresence Conductor in Cisco TMS:

If you have not already done so, in Cisco TMS go to **Administrative Tools > Locations > IP Zones** and define one IP zone per TelePresence Conductor, or per TelePresence Conductor cluster.

### Step 3 Configure conference bridge resources in TelePresence Conductor:

In TelePresence Conductor, configure one or more conference bridge pools and Service Preferences for the conference bridges to be used for scheduled conferences.

Pools and Service Preferences should only contain bridges within the same physical location.

Various configurations are possible depending on the requirements of your organization. In particular, whether you need to allocate dedicated resources just for scheduled conferences or if it is acceptable to share resources with non-scheduled conferences. The latter case has the risk that a scheduled conference may not be able to start if non-scheduled conferences have already used up the available resources.

Configuration examples are given in the Cisco Collaboration Meeting Rooms (CMR) Premises 5.0 Solution Guide, available on Cisco.com:

<http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/solutions/cmrpremises/cmr-premises-solution-guide-r5-0.pdf>

To optionally implement the Scheduling—dedicated bridge case, you must "mark" the relevant conference bridge pool(s) for scheduling use. Do this on the Service Preference page in TelePresence Conductor.

**Note** When configuring conference bridge pools dedicated for scheduling, we recommend the following:

- Give the conference bridge pool a name indicating that it should only be used for scheduled conferences.
- Check that the pool is only used in a single Service Preference
- Check that the Service Preference is not used in a CMR or ad hoc conference.

### Step 4 Allocate the TelePresence Conductor location:

Allocate the appropriate Location to each conference bridge pool defined in the previous task. Scheduled conferences do not need a dedicated Location. Use the same Location that is assigned for rendezvous conferences.

**Step 5 Configure conference templates in TelePresence Conductor:**

If a suitable conference template does not already exist in TelePresence Conductor, define one or more templates to reflect your scheduled conferencing requirements.

In TelePresence Conductor, go to **Conference configuration > Conference templates**. Set **Scheduled conference** to **Yes**.

**Step 6 Configure conference aliases in TelePresence Conductor:**

Define one or more TelePresence Conductor aliases to reflect your scheduled conferencing requirements.

In TelePresence Conductor, go to **Conference configuration > Conference aliases**.

These configuration requirements apply:

- Personal CMRs provisioned through Cisco TMSPE cannot be used for scheduled conferences.
- A dedicated conference alias is required for scheduled conferences. Do not use a conference alias that is already allocated to non-scheduled conferences.
- Set **Allow conference to be created** to **No**.

**Step 7 Configure conference aliases in Cisco TMS:**

In Cisco TMS, go to **Systems > Navigator** > select the TelePresence Conductor Aliases and select **Aliases** and select **New**.

The alias names do not have to match their corresponding conference aliases in TelePresence Conductor, but it may be administratively convenient to use the same names.

Specify the **Alias Pattern** setting to match the Incoming alias setting for the corresponding conference alias in TelePresence Conductor. (Unlike the TelePresence Conductor, the pattern is not specified as a regular expression.)

**Note** Cisco TMS aliases are assigned dynamically by TMS when it creates conferences, and can be manually modified.

**Step 8 (Optional) Edit Service Preferences in Cisco TMS:**

Unlike conference aliases, Cisco TMS automatically creates its Service Preferences. Values are populated from the Service Preference in TelePresence Conductor that is associated with the relevant alias pattern.

To optionally change Service Preference settings, in Cisco TMS, go to **Systems > Navigator > Conductor > Service Preferences** and select **Edit**.

TelePresence Conductor reports the total capacity of a Service Preference to Cisco TMS. Unless you use a single, dedicated bridge for scheduling, you may want to change the Capacity Adjustment setting from its default value of 100% and monitor the effect. This setting specifies what percentage of the total capacity will be available to Cisco TMS for scheduling conferences with this Service Preference.

You might want to set the Capacity Adjustment to greater than 100 if:

- You use cascades, and meetings tend not to cascade frequently. This could offset the potential for cascade resources to be reserved, but not actually used.
- You use resource optimization for the bridges. Cisco TMS does not take optimization into account for resources that are dedicated just for scheduled conference use. Depending on the mix of endpoints involved, the endpoints may not actually use all of the resources that get allocated to them via the Conductor template settings. Overallocating capacity may offset the potential for resources to be reserved but not actually used, if the capacity initially booked by TMS is greater than the resources actually used after optimization frees up initial resources.



Over-allocating capacity (greater than 100%) clearly increases the risk that resources will be insufficient to support all participants. To minimize that risk you could use a reserve bridge pool that isn't marked for scheduling, which oversubscribed conferences can flow into.

You might want to set the Capacity Adjustment to less than 100 in the following cases:

- Generally with shared bridges for scheduled and non-scheduled conferences, since under-allocating capacity can minimize the risk of people being unable to join due to insufficient resources.
- If meetings tend to get bigger than predicted (where invites are being forwarded or uninvited participants try to join).

**Step 9 (Optional) Add conference bridges in Cisco TMS:**

If you want to do so, there are some advantages to optionally configuring TelePresence Conductor-managed conference bridges in Cisco TMS.

**Step 10 Configure TelePresence Conductor settings in TMS:**

In Cisco TMS, go to **Systems > Navigator >** select the TelePresence Conductor and go to **Settings > Edit Settings**.

In TMS Scheduling Settings, select the booking and dialing options for the TelePresence Conductor.

- 1 Do not enable H.323 dialing in either direction.
- 2 Do enable SIP URI dialing.
- 3 Optionally, go to **Extended Settings** to configure customized conference ID ranges with a specific number range and step value.

**Step 11 Schedule the Conferences:**

**Note** This guide describes the Cisco TMS Booking > New Conference method to schedule conferences. Other methods are available, including Smart Scheduler through Cisco TMSPE, Microsoft Outlook through Cisco TMSXE, and the Cisco TMSBA Booking API.

In Cisco TMS go to Booking > New Conference and define appropriate settings for the conference:

- 1 Use the **Basic Settings** to define a conference title, connection method, conference owner, start and end time, Cisco WebEx options, and options for recurrence.
- 2 Further options are available in the **Advanced Settings** area.
- 3 Use the **Participants** tab to add users and endpoints to the conference.

When you save a conference, dial-in numbers for the conference are distributed via email to the organizer and/or participants. Updated numbers are distributed if you subsequently update a conference.





## Configure Cisco MCU and TelePresence Server

- [MCU and TelePresence Server Overview, page 71](#)
- [MCU Configuration Task Flow, page 72](#)
- [TelePresence Server Configuration Task Flow, page 77](#)

### MCU and TelePresence Server Overview

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

There are two deployment options for MCU and TelePresence Server:

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

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



**Note**

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

# MCU Configuration Task Flow

## Before You Begin

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



### Note

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

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Configure Content Mode for MCU, on page 72</a>	Required. Configure the incoming content stream to use Hybrid mode. We recommend that you configure this setting using Cisco TMS.
<b>Step 2</b>	<a href="#">Set Video and Audio Codecs, on page 73</a>	Required. WebEx requires H.264 for video and content and G.711 and G.722 for audio.
<b>Step 3</b>	<a href="#">Configure Automatic Content Handover, on page 73</a>	Required. You must enable this feature for TelePresence endpoints to share during a CMR Hybrid meeting.
<b>Step 4</b>	<a href="#">Configure the Default SIP Domain for TSP Audio, on page 74</a>	Required. Use this procedure with MCU release 4.5.
<b>Step 5</b>	<a href="#">Automatically Make Content Channel Important, on page 74</a>	Recommended.
<b>Step 6</b>	<a href="#">Configure Outgoing Transcoded Codec, on page 75</a>	Recommended.
<b>Step 7</b>	<a href="#">Configure Adaptive Gain Control, on page 75</a>	Recommended.
<b>Step 8</b>	<a href="#">Configure Audio Notifications, on page 76</a>	Recommended.
<b>Step 9</b>	<a href="#">Configure Encryption, on page 76</a>	Recommended.

## Configure Content Mode for MCU

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 Cisco TMS.

### Procedure

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

## Set Video and Audio Codecs

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

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

### Procedure

- 
- 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 make sure **H.264** is checked for the following:
    - Video codecs from MCU
    - Video codecs to MCU
  - Step 4** In the Advanced Settings section make sure **G.711** and **G.722** are checked for the following:
    - Audio codecs from MCU
    - Audio codecs to MCU
  - Step 5** At the bottom of the page, click **Apply changes**.
- 

## Configure Automatic Content Handover

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

### Procedure

---

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

## Configure the Default SIP Domain for TSP Audio

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

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

For more information, refer to the MCU online help.

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

### Procedure

---

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

## 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:

### Procedure

---

- 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**.
- 

## Configure 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.

### Procedure

---

- 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**.
- 

## Configure 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.

### Procedure

---

- 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**.

---

## Configure Audio Notifications

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

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

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

### Procedure

---

**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**.

---

## Configure 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:

### Procedure

---

**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**.

## TelePresence Server Configuration Task Flow

### Before You Begin

TelePresence Server calls to WebEx support SIP only. Make sure SIP is configured correctly on TelePresence Server. Refer to the TelePresence Server help for more information on how to configure SIP.

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Configure Locally Managed Mode, on page 77</a>	Required. For TMS to control the TelePresence Server, the TelePresence Server must be set in locally managed mode.  This applies to hardware-based TelePresence Servers only. TelePresence Server on Virtual Machine must be in remotely-managed mode for it to be controlled by Conductor.
<b>Step 2</b>	<a href="#">Configure Automatic Content Handover, on page 78</a>	Required. You must enable Automatic Content Handover for TelePresence endpoints to share during a CMR Hybrid meeting.  This applies to hardware-based TelePresence Servers only. For TelePresence Server on Virtual Machine in remotely-managed mode, it is enabled automatically through the Conductor API.
<b>Step 3</b>	<a href="#">Configure the Display Setting, on page 78</a>	Recommended. Configure the display setting so that WebEx video can be shown full size on a multiscreen endpoint.  This applies to hardware-based TelePresence Servers only. For TelePresence Server on Virtual Machine in remotely-managed mode, it is enabled automatically through the Conductor API.

## Configure Locally Managed Mode

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

**Note**

This applies to hardware-based TelePresence Servers only. TelePresence Server on Virtual Machine must be in remotely-managed mode for it to be controlled by Conductor.

**Procedure**

- 
- 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**.
- 

## Configure Automatic Content Handover

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

**Note**

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

**Procedure**

- 
- 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**.
- 

## Configure the Display Setting

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

**Note**

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

## Procedure

---

- 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**.
-





## Configure Call Control

---

- [Call Control Overview, page 81](#)
- [Cisco Expressway and TelePresence Configuration Tasks, page 82](#)
- [Configuring Cisco Unified Communications Manager, page 85](#)
- [Provisioning Endpoint Display Names, page 90](#)

### Call Control Overview

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

There are four possible call control scenarios:

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

**Note**

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

## Cisco Expressway and TelePresence Configuration Tasks

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

### Before You Begin

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

- Cisco TelePresence Video Communication Server (Cisco VCS) or Expressway must be running firmware X8.5 or a later release.
- Cisco VCS Expressway or Expressway must be assigned a static IP address, DNS and NTP information, and be accessible for management via its web interface.
- Rich media licenses must be installed on the Cisco Expressway Series
- From software Version X8.5.3 we recommend that you configure the default SIP TCP timeout value in the Cisco Expressway / Cisco VCS as described in 'Reduce Default SIP TCP Timeout in Cisco Expressway / Cisco VCS' in [Requirements, on page 35](#),
- Endpoints in the network are registered to Cisco VCS Control or Expressway and/or Unified Communications Manager

**Note**

If endpoints are registered to Unified Communications Manager, you must configure a SIP trunk between Unified Communications Manager and Cisco VCS Control. For more information, refer to [Configuring Cisco Unified Communications Manager, on page 85](#).

- Firewall must have port 5061 open to allow access to Cisco VCS Expressway

If this port is not configured correctly, calls will not take place correctly.

**Note**

**IMPORTANT:** Stateful packet inspection used in Check Point Software Technologies, Inc. firewalls is incompatible with Cisco VCS Expressway and Expressway-E.

- As a result, it is highly recommended to disable SIP and H.323 application layer gateways on routers/firewalls carrying network traffic to or from a VCS Expressway or Expressway-E, because, when these are enabled they can negatively affect the built-in firewall/NAT traversal functionality of the VCS

- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network
- Cisco VCS Control or Expressway-C is in the private network
- Cisco VCS Expressway or Expressway-E is in the DMZ and has access to the Internet
- Set zones and pipes appropriately (according to your network's requirements) to allow a minimum of 2-4 Mbps for WebEx calls. For more information about bandwidth controls, please refer to the "Cisco VCS Administrator Guide" at:

<http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-maintenance-guides-list.html>

or "Cisco Expressway Administrator Guide" at:

<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html>

- If endpoints are registered to Cisco VCS Control, it must be configured as the SIP Registrar/H.323 gatekeeper.

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

Configuring Cisco VCS Control as a SIP registrar is done by configuring one or more SIP domains. The Cisco VCS Control will act as a SIP Registrar and Presence Server for these domains, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

For details on how to configure SIP domains in Cisco VCS Control, refer to the "Cisco VCS and CUCM Deployment Guide" at:

<http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html>

or "Cisco Expressway and CUCM via SIP Trunk Deployment Guide" at:

<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>

- 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 H.323 SRV records in place that resolve to the Cisco VCS Expressway for your configured SIP Domain so TelePresence participants can route to your Cisco VCS Expressway.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Create a New DNS Zone, on page 84</a>	Required. Configure a DNS zone on the Cisco VCS Expressway for connection to the WebEx cloud.
<b>Step 2</b>	<a href="#">Configure Traversal Zones for MCUs, on page 85</a>	Configure traversal zones to support MCUs that have encryption enabled (the default setting).

## Create a New DNS Zone

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

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

### Procedure

**Step 1** Create a new DNS zone: Set H.323 to **Off**.

- a) Set SIP Media encryption mode to **Force encrypted**.
- b) Turn on TLS Verify mode.
- c) In the TLS verify subject name field, enter **sip.webex.com**.
- d) 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:

[http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config\\_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.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 Cisco VCS Expressway. It must be a CA-level certificate name issued by a public CA that is supported by WebEx.

**Note** Self-signed certificates are NOT supported.

For a list of supported certificates and details on how to configure a certificate on Cisco VCS Expressway, refer to: [Configure Certificates on Cisco Expressway-E and Cisco VCS Expressway](#), on page 95.



## Configure Traversal Zones for MCUs

This procedure 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.

**Note**

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

To support MCUs that have encryption enabled, do the following

**Procedure**

- 
- Step 1** Set up a new traversal client zone from Cisco VCS Control to Cisco VCS Expressway.  
**Note** Make sure the new zone uses a different port number.
- Step 2** Configure the media encryption setting on the traversal client to be **Force unencrypted** or **Best effort**.
- Step 3** On Cisco VCS Expressway, set up a new traversal server zone that connects to the Cisco VCS Control traversal zone set up in the previous step.
- Step 4** In this new Cisco VCS Expressway traversal server zone, set media encryption to **Force unencrypted**.
- Step 5** On Cisco VCS Control set up a search rule (at higher priority than the search rule that uses the default traversal zone) that matches WebEx traffic e.g. match = `.*@example.webex.com`  
**Note** The above configuration ensures that whether the MCU encryption is enabled or not, that the video and the presentation stay on separate channels. It also ensures the content from WebEx is not encrypted when sent to the MCU (even though it is encrypted across the internet).
- 

## Configuring Cisco Unified Communications Manager

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

This section describes the following tasks:

- [Configuring Cisco Unified Communications Manager, on page 85](#)
- [SIP Trunks Between Cisco Unified Communications Manager and Cisco Expressway-C or Cisco VCS Control, on page 86](#)
- [Configuring Early Offer for SIP Messaging, on page 86](#)

- [Configuring a Routing Rule for Bridges Trunked to Unified Communications Manager](#), on page 89

## Cisco Unified Communications Manager Configuration Prerequisites

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

- Unified Communications Manager 10.5(2)SU1 or SU2
- Endpoints in the network are registered to Unified Communications Manager
- Conferencing Bridge(s) to be used (MCU or Cisco TelePresence Server) are already operational within the network and trunked to Unified Communications Manager or registered to VCS
- Cisco Expressway-C or Cisco VCS Control is deployed in the private network
- To ensure optimum SIP audio and video connectivity between MCU and TelePresence Server endpoints on Unified Communications Manager and the WebEx cloud, it is recommended to set region to permit a minimum of 2-4 Mbps.
- Cisco Expressway-E or Cisco VCS Expressway is configured with the DNS zone.

## SIP Trunks Between Cisco Unified Communications Manager and Cisco Expressway-C or Cisco VCS Control

This section describes how to configure the Cisco Expressway Series X8.5 or later and Cisco Unified Communications Manager (Unified Communications Manager versions 10.5(2)SU1 or later) to interwork via a SIP trunk.

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

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

<http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html>

## Configuring Early Offer for SIP Messaging

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

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

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

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

**Note**

The default configuration for Unified CM trunks is Delayed Offer.

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

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

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

Some specific points apply in various deployment scenarios:

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

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

- Unified Communications Manager to Cisco Expressway-C
- Unified Communications Manager to the TelePresence Conductor

## Scenario 2. Configuring Early Offer in a multi-cluster system (TelePresence Conductor connected to Unified Communications Manager SME)

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

- Unified Communications Manager SME to Cisco Expressway-C
- Unified Communications Manager SME to the TelePresence Conductor

**Note**

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

### Scenario 3. Configuring Early Offer in a multi-cluster system (TelePresence Conductor connected to Unified Communications Manager SME)

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

- Unified Communications Manager SME to Cisco Expressway-C
- Leaf Unified Communications Manager clusters to the TelePresence Conductor
- Leaf Unified CM clusters to the Unified Communications Manager SME

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

#### Procedure

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

### Fallback to Delayed Offer

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

## Endpoints

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

## Configuring a Routing Rule for Bridges Trunked to Unified Communications Manager

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

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

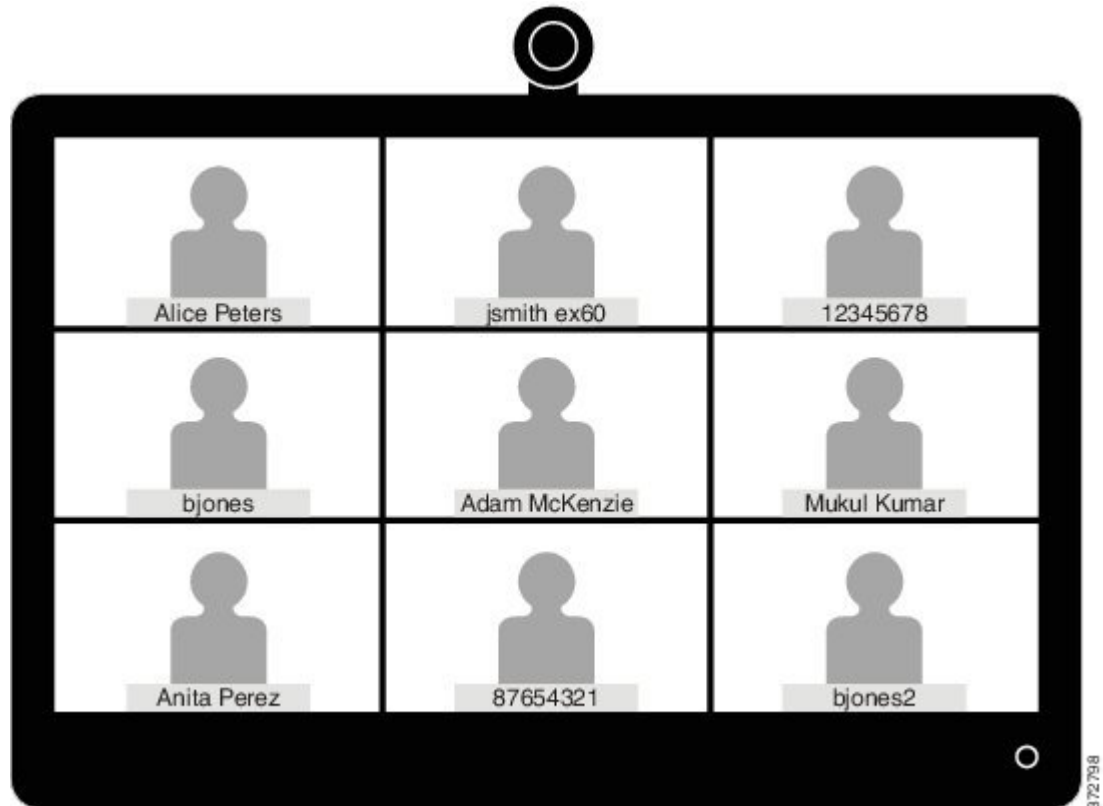
To ensure calls are routed correctly, set up a SIP routing pattern in Unified CM for your site to route to the SIP trunk for Expressway-C. For details, refer to the Unified CM documentation.

Also, make sure that the trunk for each MCU or TelePresence Server trunked to Unified CM has Early Offer enabled, as described in [Configuring Early Offer for SIP Messaging](#), on page 86.

## Provisioning Endpoint Display Names

Display names are used across endpoints such as TelePresence to identify a user to other participants.

*Figure 7: Display Names Example*



The preferred format for this name is to use the first name and last name of the user, for example Alice Peters, or the canonical name of the conference room where the endpoint is installed, such as MDR21-3-#120 (room 120 on the 3rd floor of building 21 in Madrid). However if this name is not explicitly provisioned then the system will choose the display name based on the SIP URI or device number of the endpoint. The result that is displayed will depend on how the particular users and rooms have been provisioned. This can lead to inconsistencies in the names displayed on a conference call, with the individual user information being displayed in different formats, as shown in the example above.

To ensure that names display consistently, these settings need to be provisioned in Unified CM and/or in Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) for Cisco VCS registered endpoints.

If the endpoints you want to provision are Unified CM registered, see [Provisioning Display Names on Unified CM, on page 91](#). If the endpoints you want to provision are Cisco VCS registered, see [Provisioning Display Names on Cisco VCS, on page 93](#).

## Provisioning Display Names on Unified CM

This section describes how to update display names in the Cisco Unified CM Administration user interface. It describes how users, devices, and lines are configured in order to allow an administrator to identify the correct fields and locations in which to make those updates, so that the names display correctly. The section titled [Trunks, on page 92](#) describes some optional advanced settings that may be useful to some users.

### Users and Devices

On the Cisco Unified CM Administration user interface new users are configured in the User Management > End User window. It is possible to both create new users or to import them through Active Directory (AD) or LDAP.

New devices are configured in the **Device > Phone** window. Users are then associated to a device. The details supplied during this configuration will not be used for display name purposes. The display name must be manually configured on the line under **Call routing > Directory Number**, or by selecting the line configured on the endpoint under **Device > Phone > Line#**.

### Line

Display names are configured on the line that is associated with the device. In this way, the display name is set for a particular device to which that user is associated. In the case of shared lines, it is possible to set different display names on each appearance of the shared line. However, it is recommended that the same display name be used across all devices using the first name and the last name of the user or the name of the conference room.

## Set Display Names for Unified CM Registered Endpoints using Bulk Administration

Bulk Administration can be used to set the display names for Unified Communications Manager registered endpoints for large numbers of users.

### Before You Begin

Ensure that you have users configured and associated to devices. For more information on provisioning users, see [Cisco Unified Communications Manager Administration Guide, Release 10.0\(1\)](#).

### Procedure

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | To export user records, see Export User Records in <a href="#">Cisco Unified Communications Manager Cisco Unified Communications Manager Administration Guide, Release 10.0(1)</a> . |
| <b>Step 2</b> | In the CSV file you have downloaded, copy the first name and last name columns into a new CSV file.  |
| <b>Step 3</b> | To upload this CSV file to the correct device, see Update phones using custom file in <a href="#">Cisco Unified Communications Manager Administration Guide, Release 10.0(1)</a> .   |
-

## Manually Set Display Names for Unified CM Registered Endpoints

This procedure explains how to configure the display name for a device that is registered to Unified Communications Manager, whether the device is assigned to a user who is associated with a device, or the device is a shared conference room device.

### Before You Begin

Ensure that you have users configured and associated to devices. For more information on provisioning users, see [Cisco Unified Communications Manager Administration Guide, Release 10.0\(1\)](#).

### Procedure

- 
- Step 1** Log in to the Cisco Unified CM Administration user interface and choose **Device > Phone** to go to the Find and List Phonewindow.
  - Step 2** Choose the **Device Name(Line)** for the device you want to configure to get to the Phone Configuration window for that device.
  - Step 3** Choose the line for the device from the Association area on the left hand side of the window. This brings you to the Directory Number Configuration window.
  - Step 4** In the *Directory Number Information* area, enter the display name in the **Alerting name** and **ASCII (Caller ID)** fields. **Note:** This will be used to display the user's name when communicating with devices that are not in the Unified Communications Manager cluster.
  - Step 5** In the Line 1 on Device area, enter the display name in the **Display (Caller ID)** and **ASCII Display (Caller ID)** fields. **Note:** This will appear on devices which are on the same cluster as the Cisco Unified CM.
  - Step 6** If this is a shared line, to ensure changes appear on all devices, check the **Update Shared Device Settings** check box, and click **Propagate selected**. **Note:** Cisco recommends that the display name set in the Alerting Name, ASCII Alerting Name, Display (Caller ID) and ASCII Display (Caller ID) field be the user's full name (for example First Name Last Name), for devices that are associated with a user, or the name of the conference room for endpoints that are in shared conference room spaces.
  - Step 7** Click **Save**.  
The changes are automatically propagated and will take effect immediately, unless the endpoint is on an active call, in which case they will take effect immediately after the active call has ended.
- 

## Trunks

If required, the following features can also be configured to further control the behavior of display names. These settings are on the Trunk Configuration window.

- In the Device Information area, checking the **Transmit UTF-8 for Calling Party Name** check box will transmit the ASCII Alerting Name on devices that support UTF-8.
- It is possible to hide display names on a per-trunk basis. This is done in the Inbound Calls area by selecting Restricted from the **Connected Name Presentation** drop-down list.
- In the Caller Information area, individual device display names can also be overridden by setting the **Caller Name** field.



## Provisioning Display Names on Cisco VCS

On Cisco VCS there are two methods which can be used to provision display names.

In the first method, Display Names are provisioned using FindMe templates. This method is used to provision individual users. Each template contains the details for each individual user, including their Display Name.

In the second method, Display Names are provisioned using the Direct Manage method. This method is used to provision Conference Room endpoints. This means that each Display Name is individually provisioned for each Conference Room endpoint on the endpoint itself.

### FindMe

FindMe is a Cisco TMSPE feature which allows users to specify which video and audio devices should ring when someone calls their ID. As a result, a single ID can be used to reach multiple devices which are associated with that ID.

In FindMe the administrator provisions users with FindMe accounts and provisioning templates that contain attributes, including the display name. Users can be newly added or imported using AD or LDAP.

For more information on FindMe, see Deploying FindMe in [Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide](#).

### Setting Caller ID Display Names for Cisco VCS Users

This section describes how to manually set display names for Cisco VCS FindMe users.

**Note**

If you are dealing with large numbers of users we recommend that you import their details using Active Directory or LDAP. Using this method, user display names are imported and set automatically.

#### Before You Begin

Ensure that you have installed and provisioned Cisco TMSPE. See [Configuring Cisco VCS for provisioning, Installing Cisco TMSPE, and Setting up users and provisioning in Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide](#).

#### Procedure

- 
- Step 1** Log in to Cisco TMS, go to **Systems > Provisioning > Users**.
- Step 2** In the **User Settings** pane, click **Edit**. The **User Settings** dialog box opens.  
In the **Display Name** field, enter the first name and last name of the user. **Note:** If the user has been imported using LDAP, the Display Name will be already associated with the user.
-

## Setting Caller ID Display Names for Conference Rooms

### Procedure

---

- Step 1** Log in to Cisco TMS, go to **Systems > Provisioning > Users**.
- Step 2** In the Navigator, choose the conference room you want to update from the pane on the left side of the window.
- Step 3** Choose the Address of the endpoint that you want to configure. This will bring you to the user interface of the endpoint that you have chosen.
- Step 4** Choose **Configuration > System Configuration**, and search for the word 'display' using the search field on the left side of the window.
- Step 5** Enter the Display Name in the **Profile 1 DisplayName** field. **Note:** Steps 4 and 5 may vary depending on the endpoint model you have chosen.
- Step 6** Click **Save**.
-



# Configure Certificates on Cisco Expressway-E and Cisco VCS Expressway

- [Supported Certificates](#), page 95
- [Certificate Configuration Tasks](#), page 96

## Supported Certificates

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



### Note

Self-signed certificates are NOT supported.

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

- entrust\_ev\_ca
- digicert\_global\_root\_ca
- verisign\_class\_2\_public\_primary\_ca\_-\_g3
- godaddy\_class\_2\_ca\_root\_certificate
- Go Daddy Root Certification Authority - G2
- verisign\_class\_3\_public\_primary\_ca\_-\_g5
- verisign\_class\_3\_public\_primary\_ca\_-\_g3
- dst\_root\_ca\_x3
- verisign\_class\_3\_public\_primary\_ca\_-\_g2
- equifax\_secure\_ca

- entrust\_2048\_ca

To use a certificate generated by entrust\_2048\_ca with Cisco VCS Expressway upgraded from X7.2, you must replace the Entrust Root CA certificate in the trusted CA list on the Cisco VCS Expressway with the newest version available from Entrust. You can download the newer entrust\_2048\_ca.cer file from the Root Certificates list on the Entrust web site at [https://www.entrust.net/downloads/root\\_index.cfm](https://www.entrust.net/downloads/root_index.cfm).

- verisign\_class\_1\_public\_primary\_ca\_-\_g3
- ca\_cert\_signing\_authority
- geotrust\_global\_ca
- GlobalSign Root R1

**Note**

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

- thawte\_primary\_root\_ca
- geotrust\_primary\_ca
- addtrust\_external\_ca\_root

This list may change over time. For the most current information, contact WebEx or review the information at the following link: [https://cisco-support.webex.com/guest/articles/en\\_US/Usability\\_FAQs/WBX83490/myr=false](https://cisco-support.webex.com/guest/articles/en_US/Usability_FAQs/WBX83490/myr=false)

**Caution**

Wildcard certificates are not supported on Cisco VCS Expressway.

## Certificate Configuration Tasks

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Generate a Certificate Signing Request (CSR), on page 97</a>	
<b>Step 2</b>	<a href="#">Install the SSL Server Certificate, on page 97</a>	Use this procedure to install the SSL server certificate on Cisco Expressway-E or Cisco VCS Expressway.
<b>Step 3</b>	<a href="#">Configure the Trusted CA List, on page 98</a>	The version of Cisco VCS Expressway or Cisco Expressway-E that you are using will determine how you configure the trusted CA certificate list. This section

	Command or Action	Purpose
		provides procedures if you have upgraded Cisco VCS Expressway or if you have freshly installed Cisco VCS Expressway or Cisco Expressway-E.

## Generate a Certificate Signing Request (CSR)

To generate a certificate signing request, do the following:

### Procedure

- 
- Step 1** In Cisco Expressway-E or Cisco VCS Expressway go to **Maintenance > Security certificates > Server certificate**.
- Step 2** Click **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 along with a message indicating that CSR creation was successful.
- Note** The private key is automatically generated as part of the CSR creation process. DO NOT click the option to Discard CSR, because this will force you to regenerate the CSR and will discard the previously generated private key.
- 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**.
- Note** Most certificate authorities will require the CSR to be provided in a PKCS#10 request format.
- Step 5** Submit the CSR to your public CA.
- Note** Make sure your public CA provides you with an SSL server certificate that includes both Server and Client Auth keys.
- Once you receive the SSL server certificate from your public CA, you are ready to install it on the Cisco Expressway-E or Cisco VCS Expressway
- 

## Install the SSL Server Certificate

Use this procedure to install the SSL server certificate on Cisco Expressway-E or Cisco VCS Expressway.

### Before You Begin

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

**Caution**

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

**Procedure**

- 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).  
You may also want to verify the validity of the server certificate by opening it as a .CER file. Here you should observe that the Issued to field is that of the Cisco Expressway-E or Cisco VCS Expressway server.
- 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 Cisco Expressway-E or Cisco VCS Expressway 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**.  
After uploading the server certificate, you'll see a message at the top of the page indicating that files were uploaded.

## Configure the Trusted CA List

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Stack the Intermediate Certificate CA Certificate, on page 99</a>	In some cases, root CAs will use an intermediate CA to issue certificates. If the server certificate is issued by an intermediate CA, then you will need to add the intermediate CA certificate to the default Trusted CA list.  This procedure applies to Cisco VCS Expressway X7.2.3 only.
<b>Step 2</b>	<a href="#">Trusted CA Certificate List Configuration Tasks for Upgrades, on page 100</a>	If you upgraded your Cisco VCS Expressway from X7.2.3 to X8.5, the trusted CA certificate list from X7.2.3 will be retained. Use the procedures in this section to reset the trusted certificate list or to add an intermediate CA certificate.
<b>Step 3</b>	<a href="#">Trusted CA Certificate List Configuration Tasks for New Installations, on page 103</a>	If you are using a freshly installed Cisco Expressway-E or Cisco VCS Expressway X8.5, 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.

	Command or Action	Purpose
		In addition, you will need to add the root certificate used by the WebEx cloud to the default trusted CA certificate list on your Cisco Expressway-E or Cisco VCS Expressway X8.5, which is DST Root CA X3.

## Stack the Intermediate Certificate CA Certificate

Use this procedure with Cisco VCS Expressway X7.2.3.

In some cases, root CAs will use an intermediate CA to issue certificates. If the server certificate is issued by an intermediate CA, then you will need to add the intermediate CA certificate to the default Trusted CA list.

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

### Procedure

- Step 1** Open the server certificate as a .CER file.
- Step 2** Click the **Certification Path** tab, then double-click the **Intermediate Certificate**. This opens 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 then click **Finish**.
- Step 8** Copy the default Trusted CA list from the Cisco VCS Expressway by going to **Maintenance > Certificate management > Trusted CA certificate** and clicking **Show CA Certificate**. In the window that opens, select all contents.
- 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)  
**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**.  
Certificate configuration on Cisco VCS Expressway X7.2.3 is complete.

## What to Do Next

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

[https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config\\_guide/Cisco\\_VCS\\_Certificate\\_Creation\\_and\\_Use\\_Deployment\\_Guide\\_X7-2.pdf](https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Certificate_Creation_and_Use_Deployment_Guide_X7-2.pdf)

## Trusted CA Certificate List Configuration Tasks for Upgrades

If you upgraded your Cisco VCS Expressway from X7.2.3 to X8.5, the trusted CA certificate list from X7.2.3 will be retained.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Reset the Trusted CA Certificate List, on page 100</a>	If the default trusted CA certificate list is not currently in use, we recommend that you reset it back to the default CA Certificate. This simplifies the process of ensuring that the required certificates are in place.
<b>Step 2</b>	<a href="#">Update Certificates on Cisco Expressway-E or VCS Expressway X8.5, on page 101</a>	
<b>Step 3</b>	<a href="#">Add the Intermediate Certificate CA Certificate, on page 102</a>	In some cases, root CAs will use an intermediate CA to issue certificates. If the server certificate is issued by an intermediate CA, you must add the intermediate CA certificate to the default Trusted CA list.

## Reset the Trusted CA Certificate List

Use this procedure on Cisco VCS Expressway Upgraded from X7.2.3 to X8.15.

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

To reset the trusted CA certificate list on the Cisco VCS Expressway X8.5, do the following:

### Procedure

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

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



The default trusted CA certificate list on the Cisco 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 Cisco VCS Expressway.
- Step 3** Search for the root CA that issued the server certificate.  
If the server certificate is issued by the top level root CA and NOT by an intermediate CA and the valid root CA certificate is present in the default trusted CA certificate list, then certificate configuration on the Cisco VCS Expressway is complete.  
If the server certificate is issued by an intermediate CA or if the certificate for the top-level root CA that issued your server certificate is not part of the trusted certificate list, you must add it to the list, as detailed in the next section.

## Update Certificates on Cisco Expressway-E or VCS Expressway X8.5

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

### Procedure

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

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

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

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

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

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

#### *Expiration Dates of VeriSign and QuoVadis Certificates*

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

#### **Add the Intermediate Certificate CA Certificate**

Use this procedure to add the intermediate certificate CA certificate to Cisco VCS Expressway X8.15 or later.

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

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

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 that you are stacking the correct intermediate CA certificate.

#### **Procedure**

- Step 1** Open the server certificate as a .CER file.
- Step 2** Click the **Certification Path** tab.
- Step 3** Double-click the **Intermediate Certificate**.  
This opens 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 then click **Finish**.
  - Step 9** Change the extension of your intermediate CA certificate from .cer to .pem. For example: intermediate.pem
  - Step 10** In Cisco VCS Expressway X8.5, 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 Cisco VCS Expressway X8.5 is complete.

### What to Do Next

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

- [http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config\\_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf](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)
- [http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config\\_guide/X8-5/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-5.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-5.pdf)

## Trusted CA Certificate List Configuration Tasks for New Installations

If you are using a freshly installed Cisco Expressway-E or Cisco VCS Expressway X8.5, you will need to load your own list of trusted CA certificates, because it does not (by default) contain any certificates in its default trusted CA certificate list.

In addition, you will need to add the root certificate used by the WebEx cloud to the default trusted CA certificate list on your Cisco Expressway-E or Cisco VCS Expressway X8.5, which is DST Root CA X3.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Add the DST Root Certificate, on page 104</a>	Your Cisco Expressway-E or Cisco VCS Expressway must trust the certificate issuer of the server certificate that is passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud, which is DST Root CA.
<b>Step 2</b>	<a href="#">Update Certificates on Cisco Expressway-E or VCS Expressway X8.5, on page 101</a>	
<b>Step 3</b>	<a href="#">Add the Root or Intermediate Certificate CA Certificate, on page 105</a>	For the WebEx cloud to trust the Cisco Expressway-E or Cisco VCS Expressway server certificate, you must add the root or intermediate CA certificate for the CA that issued your server certificate.

	Command or Action	Purpose
--	-------------------	---------

### Add the DST Root Certificate

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

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

#### Procedure

- 
- Step 1** Go to: [http://www.identrust.com/doc/SSLTrustIDCAA5\\_DSTCAX3.p7b](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 Cisco Expressway-E or Cisco VCS Expressway X8.5, go to **Maintenance > Security certificates > Trusted CA certificate**.
- Step 6** Click **Browse**, select the DST Root certificate that you saved in step 4, and click **Open**.
- Step 7** Click **Append CA certificate**.
- 

### Update Certificates on Cisco Expressway-E or VCS Expressway X8.5

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

#### Procedure

- 
- Step 1** Go to each of the following links, copy and paste the contents of the displayed certificate into individual text files and save each with the file extension of .PEM:
- a) [VeriSign Class 3 Public Primary CA](#)
  - b) [VeriSign Class 3 Primary CA - G5](#)
  - c) [VeriSign Class 3 Public Primary CA - G3](#)
  - d) [QuoVadis Root CA 2](#)
- For example, the first one would be: **Class-3-Public-Primary-Certification-Authority.pem**
- Note:** If you are NOT using Certificate Revocation or do NOT have a Certificate Revocation policy active on your VCS-Expressway or Expressway-E device, skip to step 3.

**Step 2** If you are using 'automatic' certificate revocation, temporarily disable it:

- a) On the VCS/Expressway, go to: **Maintenance > Security certificates > CRL Management**.
- b) Set automatic CRL updates to *disabled*.

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

**Step 3** In Cisco Expressway-E or Cisco VCS Expressway X8.5, go to **Maintenance > Security certificates > Trusted CA certificate**.

**Step 4** Click **Browse**, select the first certificate that you saved in step a, and click **Open**.

**Step 5** Click **Append CA certificate**.

**Step 6** Repeat steps 4 and 5 for the other certificates you saved in step 1.

**Step 7** Re-enable 'automatic' certificate revocation, if you disabled it in step 2.

#### *Expiration Dates of VeriSign and QuoVadis Certificates*

<b>Certificate</b>	<b>Expiration Date</b>
VeriSign Class 3 Public Primary CA	Wednesday, August 02, 2028 3:59:59 PM
VeriSign Class 3 Primary CA - G5	Wednesday, July 16, 2036
VeriSign Class 3 Public Primary CA - G3	Wednesday, July 16, 2036 3:59:59 PM
QuoVadis Root CA 2	November 24, 2031

#### **Add the Root or Intermediate Certificate CA Certificate**

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

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

To add the root or intermediate CA to Cisco Expressway-E or Cisco VCS Expressway X8.5, do the following:

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

#### **Procedure**

**Step 1** Open the server certificate as a .CER file.

**Step 2** Click the **Certification Path** tab.

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

**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 then click **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 Cisco Expressway-E or Cisco 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 Cisco Expressway-E or Cisco VCS Expressway X8.5 is complete.

**What to Do Next**

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to *Cisco VCS Certificate Creation and Use Deployment Guide (X8.5)* at the following location:

- [http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config\\_guide/X8-5/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-5.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-5.pdf)



## CHAPTER

# 11

## Configure Cisco TelePresence Management Suite

---

- [Prerequisites, page 107](#)
- [Configuring the Cisco WebEx Feature in Cisco TMS, page 108](#)
- [Configuring WebEx Users in Cisco TMS, page 109](#)
- [Configuring Port Reservations for MCU and TelePresence Server in Cisco TMS, page 112](#)
- [Configuring Hybrid Content Mode for MCU in Cisco TMS, page 113](#)
- [Configuring Lobby Screen in Cisco TMS, page 114](#)
- [Configuring Conference Settings in Cisco TMS, page 115](#)
- [Configuring Single Sign On in Cisco TMS, page 118](#)

## Prerequisites

- Cisco TMS software release 14.6 is required (15.0 is recommended).
- Cisco TMSXE software release 4.1 or later is required (5.0 is recommended), 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 1.4 or later is required (1.5 is recommended), if using Smart Scheduler to schedule meetings
- MCU calls to WebEx support SIP only. The following settings must be configured for SIP:
  - In Cisco TMS: Allow Incoming and Outgoing SIP URI Dialing must be set to Yes in the Cisco TMS Scheduling Settings for each MCU used for CMR Hybrid meetings.

- For MCU and TelePresence Server, see [Configure Cisco MCU and TelePresence Server](#), on page 71 for more information.
- To get the new WebEx Productivity Tools features in WebEx Meeting Center WBS30, the following are required:
  - TMS 15.0
  - TMSXE 5.0

For more information, refer to the latest [CMR Hybrid Release Notes](#).

## Configuring the Cisco WebEx Feature in Cisco TMS

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

### Procedure

- Step 1** Go to **Administrative Tools > Configuration > WebEx Settings**.  
The WebEx Settings page appears.
- Step 2** Click **Add Site**.  
The WebEx Site Configuration page appears.

*Figure 8: Configuring a WebEx Site*

The screenshot shows the Cisco TelePresence Management Suite interface. The top navigation bar includes links for Portal, Booking, Monitoring, Systems, Phone Books, Reporting, and Admin. The main heading is 'WebEx Settings'. Below this is the 'WebEx Site Configuration' section. It contains the following fields and values:

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

At the bottom of the configuration section 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** For **TSP Audio**, select **Yes** if you are going to use TSP or PSTN audio.
- Note** If **Yes** is selected for TSP Audio, Cisco TMS will only use TSP audio. SIP audio will not work.
- Step 8** Click **Save**.
- Step 9** In the WebEx Configuration section, do the following: For **WebEx Enabled**, select **Yes**.
- For **Add WebEx To All Conferences**, select **Yes**.
  - 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](#), on page 108.

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 CMR Hybrid User in Cisco TMS](#), on page 111

- 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](#), on page 110 and [Configuring Single Sign On in Cisco TMS](#), on page 118

## Configuring Automatic User Lookup from Active Directory

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

### Configuring Active Directory Lookup in Cisco TMS

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

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

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

To configure Active Directory Lookup, do the following:

## Procedure

- 
- 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**.
  - Step 4** For information about each field, refer to the Cisco TMS Help.
  - Step 5** To configure 'Get WebEx Username from Active Directory', do the following:
  - Step 6** Go to **Administrative Tools > Configuration > WebEx Settings**.
  - Step 7** In the WebEx Configuration pane, use the Get WebEx Username from Active Directory menu to select the field in AD where you are storing the WebEx username.
  - Step 8** Click **Save**.  
For more information, refer to the Cisco TMS Help.
- 

## How WebEx Bookings Work

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

When Single Sign On (SSO) is enabled for the WebEx site, users with WebEx accounts can book WebEx-enabled meetings with Cisco TMS without requiring their WebEx password be stored in their Cisco TMS user profile. When SSO is configured and a user schedules a meeting, their WebEx username from their Cisco TMS user profile is passed to the WebEx site to complete the booking. For information about how to configure SSO, see [Configuring Single Sign On in Cisco TMS, on page 118](#).

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

## Configuring a Cisco CMR Hybrid User in Cisco TMS

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

- 'Lookup User Information from Active Directory' and 'Get WebEx Username from Active Directory' are enabled, as described in [Configuring Automatic User Lookup from Active Directory, page 6-5](#)
- Single Sign On is enabled, as detailed in [Configuring Single Sign On in Cisco TMS, on page 118](#).
- The user will use the default WebEx site for scheduling WebEx meetings

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

### Procedure

- 
- 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.  
**Note** If no WebEx site is selected, the WebEx site configured as the default will be used.
- Step 6** For WebEx Site, select the WebEx site to which the user is registered.
- 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:

### Procedure

---

- 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 the Limit Ports to Number of Scheduled Participants menu 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:

### Procedure

---

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

## Configuring Hybrid Content Mode for MCU in Cisco TMS

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

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

### Procedure

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

## Configuring Lobby Screen in Cisco TMS

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

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

### Procedure

- 
- 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 Cisco TMS. [Table 18: Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled, on page 115](#) describes what the first TelePresence participant in a meeting will see in different scenarios. To ensure that the first TelePresence participant never sees a black screen, make sure you set “Use Lobby Screen for conferences” to Yes for all TelePresence Servers you will use for CMR Cloud meetings as described in the previous section.

**Table 18: Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled**

<b>TelePresence Server Lobby Screen Setting</b>	<b>CMR Hybrid meeting?</b>	<b>At least one WebEx participant?</b>	<b>WebEx participant has camera enabled?</b>	<b>First TelePresence participant will see</b>
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 CMR Hybrid meetings.

## 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:

### Procedure

- 
- Step 1** Go to **Administrative Tools > Configuration > Conference Settings**.
- Step 2** In the Conference Create Options section, set **Default Picture Mode** to **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.

### Procedure

- 
- Step 1** Go to **Administrative Tools > Configuration > Conference Settings**.
- Step 2** In the Conference Connection/Conference Extension 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**.  
This enables TelePresence participants to 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.
  - For **Contact Information to Extend Meetings** you can 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** (Optional) You can configure the length, timing and content of the in-video warnings, by setting the following options:

- a) **Message Timeout (in seconds)** is the number of seconds that a warning message will be displayed. (Default setting is 10.)
- b) **Show Message X Minutes Before End** is the number of minutes before the end of a meeting during when 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.

**Step 4** Click **Save**.

---

## Configuring Allow Early Join

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



---

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

---

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

### Procedure

---

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

**Step 2** Click **Save**.

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

---

## Configuring Resource Availability on Extension

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

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

### Procedure

- 
- Step 1** Go to **Administrative Tools > Configuration > Conference Settings > Resource Availability Check on Extension**.
- Step 2** Click **Save**.  
This setting works in conjunction with Extend Conference Mode and applies to Automatic Best Effort or Endpoint Prompt. The options are:
- **Best Effort:** Conferences will only automatically extend beyond the scheduled end time on a best effort basis if all resources are available for the next 15 minutes.
  - **Ignore:** Cisco TMS will ignore the resource availability check, and conferences will automatically extend beyond the scheduled end time regardless of whether all the resources are available or not. The only exception to this is if the port used on the main participant clashes with another conference.
- 

## Configuring Single Sign On in Cisco TMS

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

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

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

- A TMS Site Administrator manually enters the WebEx Username in a user's profile.

When an organizer schedules a meeting with WebEx using Cisco TMS, Cisco TMS sends the meeting information to the WebEx site with that WebEx username designated as the WebEx host.



### Note

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

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

**Note**

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

When an organizer schedules a meeting with WebEx using Cisco TMS, Cisco TMS requests AD for the WebEx username of the meeting organizer using the username and password that the Cisco TMS administrator filled in on the Network Settings page for AD lookup.

When AD supplies Cisco TMS with the WebEx username of the organizer, Cisco TMS sends the meeting information to the WebEx site with that WebEx username designated as the WebEx host.

## Prerequisites

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

- Partner Name

This value must be determined by the WebEx team, because it must be unique among all WebEx customers. Contact the WebEx account team for this information.

Example: `examplesso.webex.com`

- Partner Issuer (IdP ID)

This is the Identity Provider, which is your TMS. This value must be determined by the WebEx team. Contact the WebEx account team for this information.

Cisco recommends using a name to indicate your company's TMS.

Example: `examplertms`

- 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:

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	Ensure the WebEx site on which you want to enable SSO has been created in Cisco TMS.	See <a href="#">Configuring the Cisco WebEx Feature in Cisco TMS</a> , on page 108 for details.
<b>Step 2</b>	Generate a certificate to secure the connection between Cisco TMS and the WebEx site.	See <a href="#">Generating a Certificate for WebEx</a> , on page 120 for details.
<b>Step 3</b>	Enable Partner Delegated Authentication on the WebEx site.	See <a href="#">Enabling Partner Delegated Authentication on the WebEx Site</a> , on page 124 for details.
<b>Step 4</b>	Enable SSO in Cisco TMS.	See <a href="#">Enabling SSO in Cisco TMS</a> , on page 125 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:

### Procedure

- 
- 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 file extension is either .cer or .crt 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](#).
- 

### 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:

#### Procedure

- 
- 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 either .cer or .crt and provide this Base64 PEM 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.
  - Step 4** Use this PKCS#12 file to upload to TMS in [Enabling SSO in Cisco TMS](#)
- 

### 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.

### 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:

### Procedure

- 
- 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](#).
  - Step 2** Create a Base64 PEM encoded version of the signed certificate using step 8 [Using OpenSSL to Generate a Certificate](#).
  - Step 3** Change the file extension 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](#).
  - Step 5** Use this PKCS#12 file to upload to TMS in [Enabling SSO in Cisco TMS](#).
- 

## 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:

### Procedure

- 
- Step 1** Follow the steps in [Using OpenSSL to Generate a Certificate](#).
  - 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](#).
- 

## 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:

## Procedure

- 
- Step 1** Generate a private key.
- Step 2** Generate a certificate signing request (CSR).
- Step 3** Have a certificate authority sign the CSR.
- Step 4** Make sure the extension of the signed certificate is .cer or .crt and provide it to the WebEx team.
- Step 5** Convert the signed certificate and private key into a PKCS#12 formatted file.
- Step 6** Upload the converted certificate and private key to TMS.
- Step 7** In Windows, open a command prompt.
- Step 8** Navigate to the openssl\bin installation directory.
- Step 9** Generate a private key using following command: **openssl genrsa -out tms-privatekey.pem 2048**.
- Step 10** 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 11** Enter the data requested, including:
- a) Country
  - b) State or province
  - c) Organization name
  - d) Organization unit
  - e) Common name (this is the Cisco TMS FQDN)
  - f) (Optional) Email address, password, company name
- Step 12** 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.
- Step 13** Self-sign the certificate using either OpenSSL or Windows CA:
- a) 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.
  - b) 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 14** 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.
- Step 15** If the certificate is in an email or web page and not in its own file, open the file and copy its 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 16** (Skip this step if certificate is in .pem format) 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**
- Step 17** Change the extension to .cer or .crt and provide this signed certificate to the WebEx Cloud Services team.
- Step 18** Combine the signed certificate .pem with the private key created in step 3 using the following OpenSSL command: **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

**Note** 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](#) to complete the SSO configuration.

---

## Enabling Partner Delegated Authentication on the WebEx Site

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

### Before You Begin

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.

### Procedure

---

- Step 1** Request that the WebEx Cloud Services team add a Partner Certificate for your TMS, configured for SAML 2.0 federation protocol.
- Step 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](#).
- Step 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.
- Step 4** Proceed with the section "Enabling SSO in Cisco TMS".
- Step 5** Log into your WebEx administrative site and go to **Manage Site > Partner Authentication**.



The Partner Delegated Authentication page appears.

The screenshot shows the 'Site Administration' page in Cisco TMS. The left sidebar contains a navigation menu with links like Home, Manage Site, Manage Users, Session Types, and Assistance. The main content area is titled 'Partner Delegated Authentication'. Below this, there is a section 'Partner SAML Authentication Access' with a table. The table has three columns: 'Host', 'Site Admin', and 'Partner Certificate'. The 'Host' and 'Site Admin' columns have checkboxes that are checked. The 'Partner Certificate' column shows the value 'example.sso.webex.com' and a 'View Details' link. Below the table are 'Update' and 'Cancel' buttons. At the bottom, there is a footer with copyright information and links to Privacy and Terms of Service.

Host	Site Admin	Partner Certificate
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	example.sso.webex.com <a href="#">View Details</a>

- Step 6** In the Partner SAML Authentication Access section, make sure both **Host** and **Site Admin** are checked and click **Update**.

## Enabling SSO in Cisco TMS

To enable SSO in Cisco TMS, do the following:

### Before You Begin

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.

### Procedure

- 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.

**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 9: WebEx Settings SSO Configuration in Cisco TMS**

The screenshot displays the Cisco TelePresence Management Suite interface. The top navigation bar includes links for Portal, Booking, Monitoring, Systems, Phone Books, Reporting, and Administrative Tools. The 'WebEx Settings' page is active, showing the 'WebEx Site Configuration' and 'SSO Configuration' panes. In the 'WebEx Site Configuration' pane, the 'Enable SSO' dropdown is set to 'Yes'. The 'SSO Configuration' pane shows the 'Certificate' field with the value 'WebExTestCertificate (CN=tvasset-WYS.cisco.com)' and the 'Upload Certificate' button. The 'Certificate Password' field is masked with dots. The 'Partner Name' field is 'example', 'Partner Issuer (IdP ID)' is 'tmsexample', 'SAML Issuer (SP ID)' is 'https://example.webex.com/example', and 'AuthnContextClassRef' is 'urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtecte'. The 'Save' and 'Back' buttons are at the bottom.

## Supported Configurations for Scheduling on Behalf of the WebEx Host





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

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

- WebEx site does not use SSO and TMS does not have SSO configured. No partner delegated authentication (PDA) relationship with the WebEx site. WebEx host login: The WebEx username and password are stored in WebEx, and the user authenticates directly to the WebEx site.

- TMS scheduling: The host's WebEx username and password are also stored in their TMS personal profile. This must be maintained by the user, if they have access to the TMS, or by the TMS administrator. The TMS passes both username and password to WebEx at scheduling time.
- WebEx site does not use SSO, but TMS does have SSO configured. PDA relationship with the WebEx site. WebEx host login: The WebEx username and password are stored in WebEx, and the user authenticates directly to the WebEx site.
  - TMS scheduling: The host's WebEx username is stored in a TMS personal profile (a TMS admin task) but the WebEx password is not stored in TMS. TMS is trusted to schedule for that user.
- WebEx site uses SSO, and TMS has SSO configured. PDA relationship with the WebEx site. WebEx host login: The WebEx user logs in through the SSO identity service provider.
  - TMS scheduling: The host's WebEx username is stored in a TMS personal profile (a TMS admin task) but the WebEx password is not stored in Cisco TMS. Cisco TMS is trusted to schedule for that user.

**Figure 10: Site-level WebEx SSO and TMS PDA/SSO Support Matrix for CMR Hybrid**

		SSO-integrated WebEx Meeting Center?	
		Y	N
PDA/SSO-integrated TMS?	Y		
	N		

## Guidelines for Renewing Your PDA/SSO

If you use a certificate signed by a public CA that will soon be expiring you must renew it. Using an expired certificate will cause CMR Hybrid meeting scheduling to fail as WebEx rejects an expired certificate presented by TMS on behalf of a CMR Hybrid meeting scheduling attempt.

Here are some guidelines on how to deal with an expired certificate:

- It is possible to have more than one delegated partner certificate on your WebEx site at any given time. So you may have a backup TMS and an online/active TMS each with unique certificates. Or, better yet, you may have exported the same certificate w/private key from one of those TMS instances to the alternate and they share an FQDN/hostname. [call this cold standby]. Or, you are deploying a redundant

TMS environment and you use a single certificate with multiple SAN's containing each unique TMS FQDN and a shared CN for the NLB/frontend TMS name.

- Be aware that you will want the **Issued To** or CN(CommonName) field to be unique because we can only hold one certificate at a time referring to a given **Issued To** or **CN** field.

The reason for this is that we store your certificates on your site using the **Issued To** sort order. If we find a certificate with the identical **Issued To** name as an existing certificate, we should come back to you and ask you to clarify whether or not you want the existing certificate to be REPLACED with the new one. Most likely this is the case but we can not store [2] certificates on your WebEx site with identical **Issued To** names in the certificate [CN]. If this occurs, the new certificate will not actually be loaded and functional until we delete/replace the old one with the new one. So in order to prevent this issue, please tell us to replace the old certificate with the new one OR make sure that the new certificate has different information in the **Issued To** or **CN** field. This is possible for instance if TMS were given a different FQDN [eg TMS1.company.com vs TMS2.company.com]



## Configure Cisco TelePresence Management Suite Extension for Microsoft Exchange

- [Prerequisites, page 129](#)
- [Deployment Best Practices, page 129](#)
- [Scheduling Options with Cisco TMSXE, page 130](#)
- [Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook, page 130](#)
- [Configuring Cisco TMSXE for the WebEx Scheduling Mailbox, page 134](#)

### Prerequisites

- Cisco TMSXE software release 5.2 or later is required.
- Cisco TMS software release 15.2 or later is required.
- Endpoints that are available as mailboxes for booking in a video 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:

[http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/tmsxe/install\\_guide/Cisco-TMSXE-deployment-guide-4-1.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/tmsxe/install_guide/Cisco-TMSXE-deployment-guide-4-1.pdf)

## Scheduling Options with Cisco TMSXE

- Using the WebEx Productivity Tools Plug-In for Microsoft Outlook, you add WebEx to your meeting in Microsoft Outlook.

## 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 Booking Service

### Before You Begin

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 procedure.

### Procedure

- 
- 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. 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](#).

**Note**

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.

## Configuring the Server Certificate

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

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

### Generating a CSR for IIS 7 (Windows Server 2008)

**Procedure**

- Step 1** Open the Server Manager console (**Start > All Programs > Administrative Tools > Server Manager**).
- Step 2** In the Role View, select IIS Manager (**Server Manager > Roles > Web Server > IIS Manager**).
- Step 3** Double-click **Server Certificates**.
- Step 4** In the Actions pane on the right, click **Create Certificate Request**.
- Step 5** (Important) In the "Common Name:" field, enter the Fully Qualified Domain Name (FQDN) of the DNS name which users will type into the address bar in their browser to reach your website (site.cisco.com NOT site). If you have a different physical hostname than what users will type into their browsers to get to your site, make sure to put in the name users will use.
- Step 6** In the **Organization** field, type your organization name.
- Step 7** In the **Organizational Unit** field, type the name of your organization and click **Next**.
- Step 8** In the **City/locality** field, type the city where the server resides and click **Next**.
- Step 9** In the **State/province** field, type the state where the server resides.
- Step 10** In the **Country/Region** field, select US (United States) and click **Next**.
- Step 11** Leave the CSP at the default value.
- Step 12** For the **Bit Length**, select 2048.
- Step 13** Enter (or Browse to) a filename to save the certificate request (CSR), click **Finish**.
- Step 14** Copy and paste the entire contents of the CSR file you just saved.

The default save location is C:\.

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

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

### Procedure

---

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

## Installing the Intermediate CA Certificate (If Applicable)

### Procedure

---

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

## Installing the SSL Server Certificate

### Procedure

---

- Step 1** In the IIS Manager console, go to the **Server Certificates** action pane, and click **Complete Certificate Request**. The Complete Certificate Request Wizard appears.
- Step 2** Browse to the location where you saved your SSL server certificate, select it, then click **Open**.
- Step 3** Enter a friendly name for your certificate (use the certificate's hostname if you're unsure). Then click **OK**.



At this point SSL is available for TMSXE. You will still need to configure the TMSXE or individual directories to use SSL. Select your IIS Site.

- Step 4** In the action pane on the right, under Edit Site, click **Bindings**.
  - Step 5** Click the **Add** button.
  - Step 6** In the Type menu, select **https**.
  - Step 7** In the SSL certificate menu, select your SSL certificate.
  - Step 8** Click **OK**.
- 

## Setting Up Communication Between Your WebEx Site and Cisco TMSXE

Follow the steps described in [Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account](#), on page 151.

### Configuring the Location Displayed for TelePresence Rooms in Outlook

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

#### Procedure

---

- Step 1** To display the Select Attendees and Resources Address Book window, click the **To...** button in the Meeting window.
  - Step 2** To display the Add Telepresence Rooms window, click the Add Telepresence Rooms button the Meeting Options pane.

Location in the "Select Telepresence Rooms" window is read from Active Directory upon startup of TMSXE for the Active Directory accounts of the enabled mailboxes and is provided to the WebEx and TelePresence Integration to Outlook. It is a simple text field, and not structured data. The location information is the same as what is displayed in the "Location" column in the Microsoft Exchange Address Book, shown in [Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook](#), on page 130

The structure and hierarchy displayed in the drop-down menu in the Exchange Address Book ( [Configuring Cisco TMSXE for the WebEx and TelePresence Integration to Outlook](#), on page 130) is manually created by the Exchange administrator. This can be done by creating nodes, giving them a name and a search filter. A common use (besides geographical) is to structure the list using departments, groups or business units. For more information, refer to the documentation for Microsoft Exchange.
- 

### Installing the WebEx and TelePresence Integration to Outlook

Meeting organizers who want to schedule meetings using the WebEx and TelePresence Integration to Outlook plug-in, must download and install the WebEx Productivity Tools with TelePresence from your WebEx site.

For details, refer to: [Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account](#), on page 151

## Configuring Cisco TMSXE for the WebEx Scheduling Mailbox

### Procedure

---

- Step 1** Configure the WebEx mailbox in Microsoft Exchange.
- Step 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.

### Procedure

---

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

### Procedure

---

- 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, stricken the message delivery restrictions as needed.

For example, require senders to be authenticated, only allow from people in a specific group or similar.

For more information, refer to: [Configure Message Delivery Restrictions \(Exchange 2010 Help\)](#) or [How to Configure Message Delivery Restrictions \(Exchange 2007 Help\)](#).

- Using AD Users and computers or Powershell, set the Active Directory user account to disabled.

See [Disable or Enable a User Account](#) for instructions.





## Configure TelePresence Management Suite Provisioning Extension

- [Prerequisites, page 137](#)
- [Introduction, page 138](#)
- [User Access to Cisco TMSPE, page 138](#)
- [How Smart Scheduler Works, page 139](#)
- [Limitations, page 139](#)

### Prerequisites

- Cisco TMS software release 15.0 or later must be installed.
- Cisco TMSPE software release 1.5 or later must be installed and enabled in Cisco TMS.
- WebEx must be configured on Cisco TMS.
  - Cisco WebEx option key
  - One or more WebEx sites

Single sign-on or specified WebEx credentials for each user.

Cisco highly recommends that Single Sign On is configured for Cisco TMS and WebEx for easy addition and management of users.



#### Note

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

For details on how to configure Cisco TMS, see [Configuring Single Sign On in Cisco TMS, on page 118](#).

- Smart Scheduler requires one of the following browsers:
  - Microsoft Internet Explorer - version 10 or later

- Mozilla Firefox - version 29 or later
- Apple Safari - version 7 or later for Mac OS X and iPad
- Google Chrome - version 34 or later

## Introduction

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

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

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

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



### Note

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

## User Access to Cisco TMSPE

Users with the necessary credentials can reach Smart Scheduler using:

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

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

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

## 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

### Procedure

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

## Limitations

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

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





## Configure Audio

---

- [Prerequisites, page 141](#)
- [Configuring SIP Audio for CMR Hybrid, page 142](#)
- [Configuring PSTN Audio for CMR Hybrid, page 143](#)
- [Configuring TSP Audio for CMR Hybrid, page 145](#)

### Prerequisites

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

- Cisco VCS Control/Cisco VCS Expressway must be configured.

For details, refer to: [Cisco Expressway and TelePresence Configuration Tasks, on page 82](#).

- When using Unified Communications Manager, make sure:
  - SIP trunk is configured between Unified Communications Manager and Cisco VCS Control.

For details, see [Configuring Cisco Unified Communications Manager, on page 85](#)

- Your regions are configured for G.711 and G.722.
- If configuring PSTN audio, Gateway must be registered to Cisco VCS or Unified Communications Manager.
- MCUs/TelePresence Servers must be registered to VCS.
  - No support for MCUs/TelePresence Servers trunked to Unified Communications Manager.
- Endpoints registered to VCS and/or Unified Communications Manager 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.

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

## Configuring SIP Audio for CMR Hybrid

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

This section describes the following:

- [Configuring the WebEx Site in Cisco TMS to Use SIP Audio](#), on page 142
- [Enabling Hybrid Audio on the WebEx Site](#), on page 143



### 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:

### Procedure

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

## Enabling Hybrid Audio on the WebEx Site

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

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

[https://cisco-support.secure.force.com/WebEx\\_GPL\\_WebForm](https://cisco-support.secure.force.com/WebEx_GPL_WebForm)

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

## Configuring PSTN Audio for CMR Hybrid

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

This section describes the following:

- [Configuring the WebEx Site in Cisco TMS to Use PSTN Audio, on page 143](#)
- [Enabling Hybrid Mode on the WebEx Site, on page 144](#)
- [Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx, on page 144](#)

**Note**

Cisco CMR Hybrid always dials a fully qualified E.164 number beginning with the international escape character (+). For example: +14085551212. Make sure that VCS and/or Unified Communications Manager 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:

**Procedure**

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

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

---

## Enabling Hybrid Mode on the WebEx Site

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

## Configuring PSTN Calls to Pass Through a PSTN Gateway to WebEx

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

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

- [Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco VCS, on page 144](#)
- [Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco Unified Communications Manager, on page 145](#)

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

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

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

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

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

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

[http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config\\_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf)

### Configuring for ISDN Gateways

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

**Note**

This step is required only for ISDN gateways.

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

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

**Note**

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

## Configuring PSTN Calls to Pass through a PSTN Gateway Registered to Cisco Unified Communications Manager

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

### Procedure

- 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 Communications Manager.
- Step 2** On Unified Communications Manager, create a route pattern according to your dial plan to route these types of calls to the appropriate PSTN gateway registered to Unified Communications Manager.  
For more information about configuring search rules on VCS, see *Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide*:

[http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config\\_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf)

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

[https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

# Configuring TSP Audio for CMR Hybrid

## Overview of CMR Hybrid with a WebEx Site Using TSP Audio

Using CMR Hybrid with a WebEx site that uses Telephony Service Provider (TSP) audio involves establishing an audio cascade between the TelePresence bridge (MCU/TelePresence Server) and the TSP conferencing service in order to join the two separate audio conferences. The TelePresence bridge makes an outbound PSTN

phone call to the TSP audio service, then enters a sequence of DTMF tones according to a “CMR Hybrid dial script” in order to join the audio conference like a dial in user.

WebEx determines and configures a unique dial script for each different TSP partner.


**Note**

TSP audio requires that the customer's TelePresence bridge is able to make an outbound PSTN call to establish an audio cascade between TelePresence and the TSP partner audio bridge. To ensure that the bridge can make the call, see [Configuring PSTN Audio for CMR Hybrid, on page 143](#).

At the time the meeting is scheduled, the phone number and DTMF script are passed from WebEx to the TelePresence bridge (MCU/TelePresence Server).

At the meeting start time, the bridge automatically makes an outbound PSTN phone call to the TSP audio service and follows the DTMF script to put the call into the audio conference. Once this audio cascade is established, the WebEx users and TelePresence users can hear and speak to each other.


**Note**

This outbound phone call is not made by each TelePresence endpoint. The call is made by the bridge itself. Even when there are several TelePresence endpoints in the meeting, only one audio cascade call is made.

To deploy Telephony Service Provider (TSP) audio, PSTN audio is required. Follow the steps in [Configuring PSTN Audio for CMR Hybrid, on page 143](#) and then contact WebEx cloud services to assist you with the TSP configuration.

## Prerequisites

The prerequisites for CMR Hybrid to work with a WebEx site using TSP audio are:

- The WebEx site functions properly (using TSP audio) without CMR Hybrid, with specific attention to these functions:

The WebEx attendees can successfully dial into the audio conference.

The dial-in attendee can enter his/her AttendeeID, thus “merging” the “Call In User 1” with his entry on the WebEx Participant List.

Active speaker indications work, and video switches to the active speaker.

- The TSP partner is verified by WebEx to be compatible with CMR Hybrid. This is arranged in advance directly between WebEx and the TSP partner. WebEx manages a list of TSP partners who have been verified, and that list is checked during the A2Q process before enabling a TSP site for CMR Hybrid.

This arrangement / verification between WebEx and the TSP partner includes:

Determining and testing the DTMF script that is needed for the TelePresence bridge to successfully dial into the audio conferences of that specific TSP partner under various conditions.

Determining if the DTMF script should be dialing in as the host, or as an attendee (this latter method involves the use of a signal from WebEx to the TSP partner indicating that the audio conference should be opened even without the host being present).

- The customer TelePresence bridge is able to establish an outbound PSTN phone call and, once answered, able to enter DTMF over the call.

- The WebEx host account(s) that will be used for CMR Hybrid meetings already function properly per the requirements in the first prerequisite (above), and is configured with a toll phone number in the TSP Audio Account configuration of their WebEx host account.

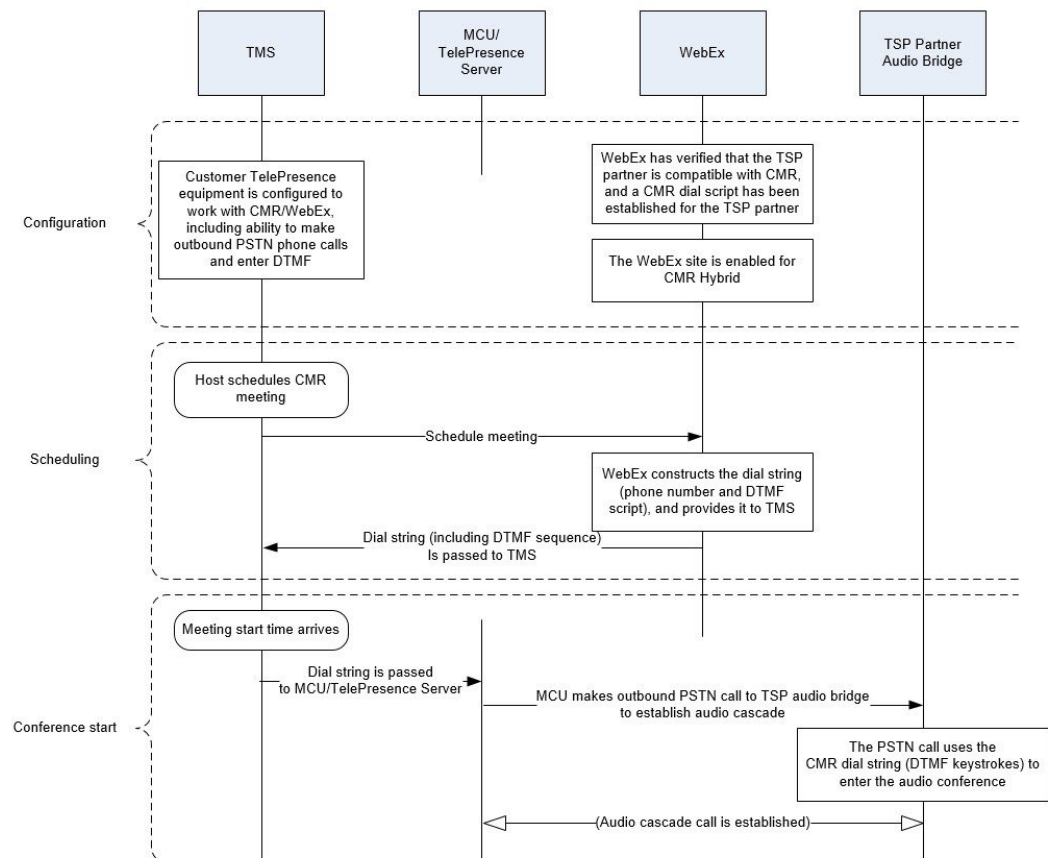
## How a TSP Meeting Works

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 When the first TelePresence participant dials in, 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.

For a detailed visual representation, refer to the diagram below.

**Figure 11: TSP Audio Configuration, Scheduling and Meeting Start Flow**



## Configuring TSP Audio for the Meeting Organizer

On a WebEx site that uses TSP audio, each WebEx host must have a TSP audio account configured in their WebEx host account. This is not specifically required for CMR Hybrid – it is necessary before the host can schedule any WebEx meeting that uses TSP integrated audio (whether or not the meeting involves CMR Hybrid is used).

If The WebEx host account(s) that will be used for CMR Hybrid meetings already function properly and is configured with a toll phone number in the TSP Audio Account configuration of their WebEx host account, this has already been done. However here is a brief description of the configuration of the TSP audio account. For details, contact your TSP partner.

### TSP Audio Account Prerequisites

Each WebEx host must have his/her own TSP audio account(s), provided by the TSP audio service provider. The TSP audio account is comprised of the information below.

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

### Configuring the TSP Audio Account of the WebEx Host Account

To configure the TSP audio account of the WebEx host account, do the following:

#### Procedure

- 
- Step 1** Open a browser and go to your WebEx site. (Example: <http://example.webex.com>)
  - Step 2** Log into the site using your WebEx host account credentials.
  - Step 3** In the upper part of the page, click **My WebEx**.
  - Step 4** In the left-hand side of the page, click **Preferences**.
  - Step 5** Click the “**Set up**” link next to the *Audio* section topic.
  - Step 6** Scroll down to the *Teleconference* section. (this will allow you to review any existing TSP audio accounts that are already configured for this host account).
  - Step 7** Click **Add account**. This will bring up the *Add Teleconferencing Account* window.
  - Step 8** In the Add Teleconferencing Account window, enter the appropriate phone numbers and access codes, as provided by the TSP audio service provider.
  - Step 9** Click **OK**.
-



**Note**

A WebEx host account can have up to three separate TSP audio accounts configured within it. If there are more than one configured, the one marked as the default account will be used for CMR meetings.

## Information about the CMR Hybrid Dial String Used for TSP Sites

The information provided here is only background information to help you understand the overall CMR Hybrid solution. The customer or CMR Hybrid deployment partner is not required to configure the dial string.

The configuration described here is determined directly between WebEx and the TSP partner as part of the TSP partner being verified as compatible with CMR Hybrid.

To connect to a meeting that uses TSP audio, the TelePresence bridge dials into the TSP partner's audio bridge and navigates the interactive voice response (IVR) audio prompt flow by using a pre-defined script of DTMF tones. Each TSP partner uses a different set of IVR menu prompts, so each TSP partner has a specific CMR Hybrid dial script.

### DTMF Dial String Example

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

- 1 Dial the phone number (this is the Toll number from the default TSP Audio Account configured within the WebEx host account for the meeting organizer).
- 2 Pause 2 seconds
- 3 Enter [participant code] DTMF values
- 4 Enter #
- 5 Pause 6 seconds
- 6 Enter #
- 7 Pause 20 seconds
- 8 Enter #1
- 9 Pause 0 seconds
- 10 Enter [attendee ID] DTMF values
- 11 Enter #

### How the Dial String is Determined

The CMR Hybrid dial script for the TSP partner contains variables which are populated using data from the default TSP audio account in the WebEx host account of the meeting organizer:

**Figure 12: WebEx Host Account / TSP Audio Account**

[Phone number]  
 [Subscriber Code]  
 [Participant Code]  
 [Attendee ID]

automatically generated

Edit Teleconferencing Account  
 Call-in toll-free number: Country/Region Number (with area/city code) 1 [redacted] [Toll-free]  
 Call-in number: Country/Region Number (with area/city code) 1 [redacted] [Toll-free]  
 Leader PIN: [redacted]  
 Conference Code: [redacted]  
 Recording dial-out number: Call-in toll-free number  
 Please select the dial-out recording number to use for network-based recording and audio broadcasts.  
 Update Cancel



## Integrate Cisco TelePresence with a Cisco WebEx Site Administration Account

---

- [Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account, page 151](#)
- [Assigning the Meeting Center TelePresence Session Type, page 153](#)
- [Network-Based Recording of CMR Hybrid Meetings, page 155](#)
- [Installing the WebEx and TelePresence Integration to Outlook, page 155](#)
- [Setting the Time Zone and Language Preferences for a User's WebEx Account, page 156](#)
- [Configuring TSP Audio for a User's WebEx Account, page 157](#)
- [Where to Go Next, page 157](#)

## Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account

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

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

- [Configuring Cisco WebEx Site Administration for CMR Hybrid, on page 151](#)
- [Assigning the Meeting Center TelePresence Session Type, on page 153](#)

## Configuring Cisco WebEx Site Administration for CMR Hybrid

To integrate Cisco TelePresence to Cisco WebEx:

## Procedure

- 
- 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**.
- 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 CMR Hybrid solution with the option to schedule meetings using the WebEx and TelePresence Integration to Microsoft Outlook, you must enter the host address for the TelePresence Management Suite Extension for Microsoft Exchange (TMSXE) in the Cisco TMS booking service URL field. (Example: `https://tmsxe.example.com/TMSService/Booking.svc`)  
For more information about configuring Cisco TMSXE, see [Configure Cisco TelePresence Management Suite Extension for Microsoft Exchange](#), on page 129
- Step 6** Click to select **List Cisco TelePresence meetings on calendar** so that scheduled meetings hosted by each user appear under **My WebEx Meetings** on their WebEx site.  
**Note** This option is removed in WebEx Meeting Center WBS29.13. TelePresence meetings will automatically appear in the list of meetings a user hosts on the WebEx site. TelePresence meetings a user is invited to are not displayed under **My WebEx Meetings**.
- 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** (TSP audio only) If deploying TSP audio, you may need to click to select **TSP identity code** and enter the code associated with your TSP (contact your TSP to determine if you need to do this, and which code you need to enter).  
**Note** TSP Call-in User merge feature should already be configured and working in regular WebEx meetings before you set up CMR Hybrid on your site.
- Step 11** In the WebEx VOIP and video connection section, select a connection method between the WebEx meeting application and the multimedia server (VoIP and video):
- **Automatically encrypted UDP/TCP SSL—(Recommended)** Allows the WebEx meeting application to connect to the multimedia server by using encrypted UDP. If the UDP connection is not allowed, the application falls back to SSL. This is the most flexible option, particularly if you need to minimize traffic congestion between the WebEx application and your telepresence devices

- **TCP SSL**—Allows the WebEx meeting application to connect to the multimedia server by using SSL. Important: TCP/SSL should ONLY be selected based on recommendation from Cisco TAC. In all other cases, UDP should be selected.

**Step 12** Optional) If you do not want users to use VoIP audio on this WebEx site, check the box **Disable Hybrid VOIP**. This disables VoIP for all meetings on the site, not only CMR Hybrid meetings.

**Step 13** Scroll to the bottom of the page and click **Save** to save your settings.

---

### What to Do Next

Proceed to [Assigning the Meeting Center TelePresence Session Type, on page 153](#) 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, on page 154](#)
- [Adding the Cisco TelePresence Session Type in the Edit User Screen, on page 154](#)

## Support for Custom Session Types

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

## Adding the Cisco TelePresence Session Type in the List of Users

### Procedure

- 
- Step 1** In the left navigation bar under **Manage Users**, choose **Edit User List**. The Edit User List screen appears.
- 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.) 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. 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 CMR Cloud.
- Note** This session type will be assigned by default when you create new host accounts by using the Add User link on a TelePresence-enabled WebEx site. The user must have this session type assigned in order to schedule CMR Hybrid meetings. If this site is an existing site updated to CMR Cloud, 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:

### Procedure

- 
- 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.
- Step 3** Required. Check the box for **PRO: Meeting Center TelePresence**, as shown circled in red in Session Types Allowed [p.1].
- 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.

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

---

## Network-Based Recording of CMR Hybrid Meetings

Meeting organizers can record CMR Hybrid meetings.

Meeting organizers can record CMR Hybrid meetings.

- The WebEx and TelePresence Integration to Outlook and WebEx Meeting Center client automatically discovers if recording is enabled and displays the appropriate message.
- Playback of a recorded meeting displays both WebEx and TelePresence video with content share, chat and polling (if enabled).
- User can navigate through recording via playback controls or clicking thumbnails of the video.
- User can see a visual representation in the recording of when participants are talking.



---

**Note** Network-based recording is enabled by WebEx Cloud Services.

---

## Installing the WebEx and TelePresence Integration to Outlook

### Before You Begin

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.

---

## Procedure

---

- 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.
- Step 9** Enter your WebEx Site URL, User Name, Password and click **Login**.
- Step 10** After logging in, the WebEx Productivity Tools communicates with the server and then you are asked to log into Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE).
- Step 11** Enter your TMSXE User name and Password and click **OK**.
- Step 12** When the message "WebEx Productivity Tools are installed" appears, click **OK**.
- Step 13** Close the Productivity Tools window.  
You can now open Microsoft Outlook and schedule CMR Cloud 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.



### Procedure

---

- 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**.
  - Step 4** If you are presented with an option to download the WebEx Productivity Tools and you have already downloaded them, click **Later**. If you wish to download and install them now, refer to step 4 of Installing the WebEx and TelePresence Integration to Outlook.  
The My WebEx Meetings page appears and in the right corner of the page, the current language and time zone settings are displayed.
  - Step 5** To change the language and time zone, click the link that displays either the current language or time zone. The Preferences page appears.
  - Step 6** Using the Time zone and Language menus, select the time zone and language you wish to use for your CMR Hybrid meetings.
  - Step 7** Click **OK**.
- 

## Configuring TSP Audio for a User's WebEx Account

Meeting organizers who need to schedule CMR Hybrid meetings that use TSP audio must add TSP audio provider information to their account.

For details, refer to Configuring TSP Audio for CMR Hybrid.

## Where to Go Next

For complete information about managing your Cisco WebEx Administration Site account, refer to the Help on your WebEx site. [https://go.webex.com/docs/T27LB/common\\_docs/en\\_US/siteadmin/help/wwhelp/wwhimpl/js/html/wwhelp.htm](https://go.webex.com/docs/T27LB/common_docs/en_US/siteadmin/help/wwhelp/wwhimpl/js/html/wwhelp.htm)





## Manage CMR Hybrid Meetings

- [Introduction, page 159](#)
- [Scheduling a CMR Hybrid Meeting , page 160](#)
- [Starting/Joining the Meeting, page 162](#)
- [Share Cisco WebEx Presentations, page 162](#)
- [Information, Tips and Known Issues About Meetings, page 163](#)

### Introduction

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

In addition to scheduling using TMS, there are up to 3 additional ways to schedule a CMR Hybrid meeting:

- Using the Cisco WebEx and TelePresence Integration to Outlook

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

For scheduling information, see [WebEx and TelePresence Integration to Outlook Quick Reference Guide](#)

For additional information, including how to schedule a meeting on behalf of another person or to assign a delegate to schedule meetings for you, refer to the WebEx and TelePresence Integration to Outlook help available in Outlook or the user guide, available on your WebEx site.

- Using the Cisco Smart Scheduler

With Cisco Smart Scheduler, Macintosh, mobile and other non-Windows users can schedule CMR Hybrid meetings using a simple web-based interface which is touch-screen friendly.

For scheduling information, refer to the [Cisco Smart Scheduler and WebEx Scheduling Mailbox Quick Reference Guide](#)

For additional information, including supported browsers and mobile platforms, refer to the Cisco TelePresence Management Suite Provisioning Extension (TMSPE) release notes.

- Using the Cisco WebEx Scheduling Mailbox

With the Cisco WebEx Scheduling Mailbox, users without the WebEx and TelePresence Integration to Outlook can create a TelePresence Enabled WebEx meeting in Outlook by inviting TelePresence rooms and then adding WebEx to the meeting by including a special invitee; the WebEx Scheduling Mailbox.

The mailbox may be called simply "webex" or something different. It 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 a CMR Hybrid Meeting

### Procedure

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

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.
- Step 11** Available participants and a planner view with their availability is displayed based on existing scheduled and ad hoc meetings. The colored vertical lines represent your current requested time for the scheduled meeting.
- Step 12** Click the tabs to have participants listed by type. If you have used scheduling before, the default tab is Last Used with quick access to the systems you have used recently.
- Step 13** Hover over any system, or the blocks in the planner view, for additional detail about the system or scheduled meeting.
- Step 14** Add participants to the meeting by selecting their checkbox and clicking the button to add them to the list of selected participants on the right side of the window. Adding network infrastructure components like MCUs and Gateways is optional as Cisco TMS will handle this for you automatically.
- Step 15** Use the External tab to add systems not managed by Cisco TMS, for example endpoints in other organizations, or telephone participants.
- Step 16** For dial-out participants, enter their contact information, and Cisco TMS will automatically connect them to the conference at the scheduled time.
- Step 17** For dial-in participants (including endpoints that do not support One-Button-to-Push), Cisco TMS will reserve the capacity needed to host the site in the conference and will provide you with precise dial-in information to forward to the participant.
- Step 18** 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 19** 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.
- Step 20** 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.  
If your WebEx site is set up to send email confirmations, you will receive two additional email notifications from WebEx: 1. An email with the subject line "Meeting Scheduled" which contains the host key and the WebEx information for the meeting 2. An email with the subject line "(Forward to attendees) Meeting Invitation" which contains only the WebEx information for attendees.

If Cisco TMS is unable to complete your booking request, 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.

In this case, try doing the following:

- 1 Edit the conference settings to try to resolve the issue and try saving the conference again.
- 2 After successfully scheduling your meeting, invite people to the meeting using your calendar application.

## Starting/Joining the Meeting

The meeting starts the following way:

- At any time, the host can join to start the meeting.
- 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.
- If the "Join Before Host" feature is enabled on the site, and the host has set Attendees Can Join Meeting Before Starting Time when scheduling the meeting using the WebEx and TelePresence Integration to Outlook, participants may join the meeting 5, 10, or 15 minutes before the scheduled time (as configured by the host). Otherwise, participants must wait for the meeting to be started by the host before they can join.
- Telepresence participants join the meeting.
  - If meeting was scheduled using Auto Connect, Cisco TMS dials and connects each supported endpoint.
  - If meeting was scheduled using One-Button-to-Push (OBTP), participants using endpoints that support OBTP press the button on their endpoint to join the meeting.
  - Participants using endpoints that don't support either Auto Connect or OBTP, join the meeting by dialing the video dial-in number listed in the meeting invitation.
- WebEx participants join the meeting by using the link in the meeting invitation.

## Share Cisco WebEx Presentations

The following procedure describes how a WebEx participant shares their presentation with TelePresence and other WebEx participants.

### Procedure

- 
- Step 1** Log into the Cisco WebEx Meeting Center application on their computers.
- Step 2** Grab the ball or be designated as presenter by the WebEx host.
- Step 3** On the Quick Start tab, click **Share Application**.
- Step 4** Start application or desktop sharing.
- Note** For a list of supported mobile clients, refer to the CMR Hybrid release notes.
-

# Information, Tips and Known Issues About Meetings

The following section contains useful information, including tips and known issues relating to CMR Hybrid meetings. The information is divided into sections corresponding to each product that is part of the CMR Hybrid 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.
- Extending a meeting is supported for both TelePresence and WebEx using the Extend Mode setting when scheduling a meeting. Meeting extension is not guaranteed. If resources (ports) are fully booked at the scheduled end time of the meeting, the meeting will end.
- A meeting organizer scheduling a meeting using the WebEx and TelePresence Integration to Outlook, should never modify that meeting later in Cisco TMS.

If the original meeting is modified later in Cisco TMS, the meeting information in Cisco TMS will fall out of sync with the meeting organizer's Outlook calendar. The reason for this is that Cisco TMSXE does not have write access to the meeting organizer's calendar and, as a result, can't make any changes to it.

## MCU and TelePresence Server

- If Conductor is used, the MCU/TelePresence Server calls into WebEx after the first TelePresence participant joins the meeting.
- If Conductor is not used, the MCU/TelePresence Server calls into WebEx at the start of the meeting, 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 Communications Manager, this can be resolved by enabling User-Agent passthrough in Unified Communications Manager.

## Cisco TMSXE

When booking a meeting using Web Scheduling Mailbox, if TMSXE detects an error condition (ex: not able to connect with WebEx server), the error email is sent in plain text format to the meeting organizer.

## WebEx

- 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.
- The WebEx host can mute all or individual participants after they join the meeting. It is not possible to mute TelePresence participants through the WebEx client. TelePresence participants must mute themselves.
- To mute WebEx participants, you have to be the WebEx host.

To reclaim the host role, you have to get the WebEx host key.

- The meeting is started by the first participant who joins the meeting (host or other WebEx participant). The rest of the participants "join" the meeting.
- 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.





## Troubleshoot CMR Hybrid

---

- [Verifying and Testing](#) , page 165
- [Troubleshooting Tips](#), page 165
- [Managing System Behavior](#) , page 176

## Verifying and Testing

### Cisco WebEx Site Administration Online Help

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

#### Procedure

---

- 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.customer-a.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 CMR Hybrid meeting:

- [Problems with Scheduling a Meeting](#), on page 166
- [Problems with Starting or Joining a Meeting](#), on page 167
- [Problems During a Meeting](#), on page 169
- [Problems with a TSP Audio Meeting](#), on page 173

- [Problems with TelePresence Server and MCU, on page 176](#)

## Problems with Scheduling a Meeting

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

See the table for troubleshooting information on how to solve common problems that prevent meetings from being scheduled correctly.

**Table 19: Problems with Scheduling Meetings**

Problem or Message	Possible Causes	Recommended Action
The meeting organizer receives no email from Cisco TMS to confirm the meeting is scheduled.	Cisco TMS configure to send confirmation email.	Check Cisco TMS configuration.  If Cisco TMS configuration is correct, check antivirus/firewall program(s) to see if they are blocking the Cisco TMS from sending.
After meeting organizer schedules a meeting using TMS, the following error is displayed: "An unexpected error occurred while communicating with WebEx." The meeting is created, but there are problems with the WebEx configuration. They receive a meeting confirmation email that contains no WebEx information.	Meeting organizer's WebEx host account is not provisioned with the Meeting Center TelePresence session type.	Log into WebEx Site Administration for your WebEx site and make sure the meeting organizer's host account has the Meeting Center TelePresence session type enabled. For more information, refer to: <a href="#">Integrating Cisco TelePresence with Your Cisco WebEx Site Administration Account, on page 151</a> .
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"> <li>• Scheduled meeting type is not One-Button-to-Push (OBTP). Only OBTP meetings appear on an endpoint.</li> <li>• Network connection failure between endpoint and Cisco TMS.</li> </ul>	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".

Problem or Message	Possible Causes	Recommended Action
<p>WebEx scheduling error in Cisco TMS (when clicking Save)</p> <p>Symptom: Cisco TMS displays 'Unable to include WebEx conference. Incorrect WebEx username or password.'</p>	<p>Network problems with WebEx site.</p> <p>WebEx user doesn't exist on WebEx site.</p> <p>Cause: WebEx site configured for this organizer does not recognize the WebEx username/password configure for the meeting organizer.</p>	<p>Check WebEx account user profile.</p> <p>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.</p> <p>Refer to Cisco TMS Troubleshooting information. This issue is not limited to Cisco CMR Hybrid.</p>
No confirmation emails from WebEx	Email is not enabled on the WebEx site	Check the WebEx site administrator.
Meeting is booked on the TMS but the WebEx does not exist.	Endpoints booked for the meeting are configured as mailboxes in Exchange but are not set to AutoAccept invitations.	Ensure that all endpoints that are available as mailboxes for booking in a Cisco CMR Hybrid meeting are set to AutoAccept in Exchange.
"We've hit a glitch in connecting to the telepresence scheduling system. Try again later."	TMSXE	Contact the TMSXE administrator.
I do not see the WebEx option when scheduling a meeting in TMS.	Your WebEx Username and Password have not been added to your TMS user profile.	Edit your TMS user and enter your WebEx username and password and then save. The WebEx option should now appear in the TMS scheduling UI.

## Problems with Starting or Joining a Meeting

This section describes possible issues meeting participants may experience when starting or joining a meeting.

Refer to troubleshooting information in the table on how to solve common problems that prevent participants from starting or joining meetings.

**Table 20: Problems with Starting or Joining Meetings**

Problem or Message	Possible Causes	Recommended Action
Can't join the WebEx meeting	Meeting hasn't started yet	wait for meeting to start

Problem or Message	Possible Causes	Recommended Action
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 did not start early (Early Meeting Start) did not work	Cisco TMS scheduled meeting does not support early start. Endpoint must wait until meeting has started to dial in.	Check Setup Buffer and Tear Down Buffer settings
Single TelePresence participant can't join the meeting	Not enough video and audio ports. Call routing issue for the endpoint to MCU or TelePresence Server	Check event log for the meeting. Also check meetings in TelePresence Server or MCU.  Administrator can lift the limit by changing the port value from the TelePresence Server Conferences page.
TelePresence participant can only join via audio only.	Not enough video ports are available.	Increase the video ports in Cisco TMS, TelePresence Server or MCU.
No TelePresence participants can join the meeting	Meeting has not started yet. Cisco TMS scheduled meeting does not support early start. Endpoint must wait until meeting has started to dial in.  Total audio and video ports for the MCU/TelePresence Server have been used up. Another cause is that the port video/audio limit for the meeting has been reached.	If total port capacity of MCU/TelePresence Server has been reached, no action is required.  For the case of the meeting limit being reached, the administrator can lift the limit from the TelePresence Server Conferences page.
MCU/TelePresence server disconnects after WebEx host joins the meeting.	WebEx host is currently joined to another meeting of which they are also the host.	Do not use the same WebEx host ID to join multiple meetings at the same time.  Only one CMR Hybrid meeting can be run per host at a time.
I do not see a CMR Hybrid meeting I was invited to under My WebEx Meetings on my WebEx site.	CMR Hybrid meetings a user is invited to are not displayed under My WebEx Meetings.	None. Only CMR Hybrid meetings that a user hosts are displayed under My WebEx Meetings.

## Problems During a Meeting

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

Refer to troubleshooting information in the table on how to solve common problems during the meeting.

**Table 21: Problems During the Meeting**

Problem or Message	Possible Causes	Recommended Action
No WebEx welcome screen	<p>Content disabled on MCU.</p> <p>Video call from MCU/TelePresence Server to WebEx failed. Call failure occurs for several reasons:</p> <ul style="list-style-type: none"> <li>• WebEx SIP dialing fails to reach destination due to unresolvable SIP URI</li> <li>• WebEx server(s) down</li> <li>• Issues with search rules in VCS</li> <li>• Media Encryption setting in VCS</li> </ul>	<ul style="list-style-type: none"> <li>• Check MCU configuration and conference status.</li> <li>• Verify search rules to ensure that SIP URI being routed correctly to WebEx site.</li> <li>• Verify encryption setting in VCS for this zone.</li> <li>• If failure persists after above actions are taken, contact WebEx site administrator.</li> </ul>
TelePresence is not linked to WebEx	<p>Video call from MCU/TelePresence Server to WebEx failed. Call failure occurs for several reasons:</p> <ul style="list-style-type: none"> <li>• WebEx SIP dialing fails to reach destination due to unresolvable SIP URI</li> <li>• WebEx server(s) down</li> <li>• Issues with search rules in VCS</li> <li>• Media Encryption setting in VCS</li> </ul>	-
Don't see video on WebEx	<p>WebEx participant does not enable video.</p> <p>WebEx participant has a problem with their camera.</p>	<ul style="list-style-type: none"> <li>• Make sure TelePresence and WebEx calls are connected.</li> <li>• Check to see if participants who joined TelePresence are sending video.</li> </ul>

Problem or Message	Possible Causes	Recommended Action
<p>Low-bandwidth warning in WebEx Meeting Center client on Windows or Mac:</p> <p>"Due to low bandwidth, we are not able to show TelePresence video at the moment"</p>	<ul style="list-style-type: none"> <li>• Not enough bandwidth is available for the WebEx Meeting Center client.</li> <li>• The downspeed drops below 180p video resolution.</li> </ul>	<ul style="list-style-type: none"> <li>• Verify there is enough bandwidth for the WebEx Meeting Center client. 1.3 mb/s of sustained throughput is required to avoid the low-bandwidth warning where datasharing is active.</li> <li>• Disconnect and reconnect to the meeting to rejoin the main video.</li> <li>• Review <a href="#">Tips for Troubleshooting Low Bandwidth with the WebEx Meeting Center Client on Windows or Mac</a>, on page 173</li> <li>• For details on Meeting Center client requirements for CMR Hybrid refer to: <a href="#">CMR Hybrid Prerequisites</a>, on page 36</li> <li>• Before contacting support, get the audio and video statistics from the meeting. In the Meeting Center client during the meeting: Select Meeting &gt; Audio &amp; Video Statistics... <ul style="list-style-type: none"> <li>◦ or in Full-Screen view, right-click the active speaker's video and select Audio &amp; Video Statistics...</li> </ul> </li> </ul>
<p>Don't see video on TelePresence</p>	-	<ul style="list-style-type: none"> <li>• Check to see if WebEx users have joined and are sending video.</li> </ul>

Problem or Message	Possible Causes	Recommended Action
Don't hear audio on WebEx	-	<ul style="list-style-type: none"> <li>• Check TelePresence call statistics and make sure TelePresence endpoint is not muted.</li> <li>• Check to see if WebEx users can hear each other.</li> </ul>
Don't hear audio on TelePresence	-	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
Don't see presentation shared from WebEx side on TelePresence side	-	<ul style="list-style-type: none"> <li>• Check TelePresence statistic for content channel status.</li> <li>• Check to see if WebEx users can see content from each other.</li> </ul>
Don't see presentation from TelePresence side on WebEx side	-	<ul style="list-style-type: none"> <li>• Check TelePresence statistic for content channel status.</li> <li>• Check to see if WebEx users can see content from each other.</li> </ul>
Don't see presentation from WebEx on WebEx side	-	<ul style="list-style-type: none"> <li>• Contact the WebEx administrator for assistance.</li> </ul>
Don't see presentation from TelePresence side on TelePresence side	-	<ul style="list-style-type: none"> <li>• Check TelePresence call statistics to see if content channel is established.</li> <li>• Try to stop the restart sending content.</li> </ul>
Presentation is displayed in main video	-	<ul style="list-style-type: none"> <li>• Check current call statistics for content channel.</li> <li>• Check to see if the SIP call encrypted.</li> </ul>

Problem or Message	Possible Causes	Recommended Action
Poor quality video from WebEx participants on TelePresence side	-	<ul style="list-style-type: none"> <li>Check network bandwidth for possible poor network connection.</li> </ul>
Poor quality audio from WebEx participants on TelePresence side	TBD	<ul style="list-style-type: none"> <li>TBD</li> </ul>
Poor quality video from TelePresence participants on WebEx side	Poor network connection	<ul style="list-style-type: none"> <li>Check call statistics for TelePresence participants.</li> </ul>
Poor quality audio from TelePresence participants on WebEx side	TBD	<ul style="list-style-type: none"> <li>TBD</li> </ul>
Audio skewed from video (lip sync issues)	In the case of PSTN/TSP audio, lip sync cannot be guaranteed	-
Active speaker does not switch in	-	<ul style="list-style-type: none"> <li>Make sure audio and video calls are linked in PSTN/TSP case.</li> </ul>
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"> <li>WebEx site administrator not configured properly.</li> <li>Audio call failed.</li> <li>If the MCU sends the wrong participant ID.</li> </ol>	<ul style="list-style-type: none"> <li>Check in Cisco TMS CCC or on MCU to see if audio call failed.</li> <li>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.</li> </ul>
Poor quality presentation from TelePresence participants on WebEx side	Possible network issue.	<ul style="list-style-type: none"> <li>Check the bandwidth between TelePresence and WebEx.</li> </ul>
Video from a WebEx participant frozen	Possible network issue.	<ul style="list-style-type: none"> <li>Check the bandwidth between TelePresence and WebEx.</li> </ul>



Problem or Message	Possible Causes	Recommended Action
Meeting ends unexpectedly	-	<ul style="list-style-type: none"> <li>• Check TelePresence log to see any cause for the call drop.</li> </ul>
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"> <li>• Check Cisco TMS booking list to confirm.</li> </ul>

## Tips for Troubleshooting Low Bandwidth with the WebEx Meeting Center Client on Windows or Mac

To troubleshoot low bandwidth with the WebEx Meeting Center client, do the following:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Review the WebEx Latency Troubleshooting Tips at: <a href="http://kb.webex.com/WBX28297">http://kb.webex.com/WBX28297</a>	
<b>Step 2</b>	Ensure you have allowed <b>all</b> specified WebEx ports for your proxy and firewall. For detailed information, refer to How Do I Allow WebEx Traffic on My Network? at: <a href="https://kb.webex.com/WBX264">https://kb.webex.com/WBX264</a>	
<b>Step 3</b>	Ensure your VCS-Expressway or Expressway-E has the correct ports enabled, by reviewing Appendix 3: Firewall and NAT settings in: <a href="#">VCS Basic Configuration (Control with Expressway) x8.2 Deployment Guide</a>	
<b>Step 4</b>	Review the TMS setting for WebEx participant bandwidth, by doing the following in TMS: Go to: <b>Administrative Tools &gt; Configuration &gt; WebEx Settings</b>	
<b>Step 5</b>	Review the site administration settings for your WebEx site, by doing the following: Log in to WebEx Site Administration for your WebEx site.	

## Problems with a TSP Audio Meeting

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

Refer to troubleshooting information in the table on how to solve common problems with TSP audio meetings.

Table 22: Problems with a TSP Meeting

Problem or Message	Possible Causes	Recommended Action
TelePresence joins audio of host's previously scheduled meeting that had run beyond the scheduled end time.	<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"> <li>Have TelePresence recite audio prompt after joining the TSP audio. "Cisco Telepresence is now in the audio conference" (or similar).</li> </ul> <p><b>Note</b> Using API method does not resolve this.</p>
TelePresence joins audio of host's previously scheduled meeting where the host had exited with the "keep audio conference running" option.	<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"> <li>Have TelePresence recite audio prompt after joining the TSP audio. "Cisco Telepresence is now in the audio conference" (or similar).</li> </ul> <p><b>Note</b> Using API method does not resolve this.</p>

Problem or Message	Possible Causes	Recommended Action
"Host private conference code" can break DTMF dumb dial entry method in some cases (dial in as host + host has already dialed in).	If the TSP has implemented a "host private conference code" (where the host uses a conference code that is not the same as the one used by the attendees, thus avoiding the need for the host to enter a PIN number), the audio prompt call flow might break the dumb-dial of the MCU if the host has already dialed into the conference. (in our testing, this is when we heard all the foreign language prompts from the TSP bridge - it was the bridge barking about the fact that the host conf code is already in use).	<ul style="list-style-type: none"> <li>• Use API method....or...</li> <li>• 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.</li> </ul>
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:</p> <pre>A2W_RspCreateConference[NBRPhoneNumber]</pre>	<ul style="list-style-type: none"> <li>• 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"> <li>1 TelePresence starts TelePresence meeting.</li> <li>2 TelePresence starts WebEx meeting.</li> <li>3 WebEx sends W2A_CreateConference to TSP.</li> <li>4 TSP sends A2W_RspCreateConference to WebEx (this would contain the TP dial string).</li> <li>5 WebEx sends dial string to MCU.</li> <li>6 MCU dials into the TSP bridge.</li> </ol> <p>The TSP API and TSP Server would need to change (among other components, of course).</p> </li> </ul>

Problem or Message	Possible Causes	Recommended Action
The TSP Audio account info, used by the MCU dial string, is obsolete.	Since the MCU collects and stores the TSP dial string at the time of meeting schedule, to be used at the time of meeting start (which can be many weeks later), there is a possibility that the dial string will be obsolete and hence the call into the TSP conference will fail. This will happen if the default (first) TSP Audio account is changed during the time between TelePresence meeting schedule and TelePresence meeting start.	<ul style="list-style-type: none"> <li>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).</li> </ul>

## Problems with TelePresence Server and MCU

This section describes possible issues with a meeting caused by TelePresence Server and MCU.

Refer to troubleshooting information in the table on how to solve common problems with TelePresence Server and MCU.

**Table 23: Problems with TelePresence Server and MCU**

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

## Managing System Behavior

### Managing the Cisco WebEx Video View Window

A window cascading effect can occur if you plug in the presentation (VGA) cable (VGA, DVI, HDMI) between your PC and your telepresence video device while you have your Cisco WebEx video view panel open. The WebEx application should detect that you have plugged into a telepresence video device and ask if you are sharing your screen via telepresence. Confirming that you are sharing avoids this cascading problem. To

prevent this issue, close the Cisco WebEx video view application before connecting your presentation cable to your laptop to present.

If you do receive a cascading screen, simply close the video view window.





# Add Cisco Unified Communications Manager Normalization Scripts

- [Normalization Script Overview](#), page 179
- [Add the Scripts](#), page 180

## Normalization Script Overview

If your deployment uses encryption and TLS on SIP trunks used for TelePresence you must add one or more of the TelePresence normalization scripts to Cisco Unified Communications Manager.



### Caution

New versions of the scripts are required for this release. To avoid unexpected call disconnects, you must ensure that the latest versions are installed.

From Cisco Unified Communications Manager Version 10.5(2), the scripts are auto-installed with the software. For earlier versions, you need to download and install the latest scripts from the Cisco website at <https://software.cisco.com/download/navigator.html?mdfid=268439621&flowid=45900>.

The following normalization scripts are available:

**Table 24: Normalization Scripts**

Script	Install . . .
telepresence-conductorinterop	SIP trunks that directly interface with a TelePresence Conductor as the next hop peer.
vcs-interop	SIP trunks that directly interface with a Cisco VCS Control or Cisco Expressway-C as the next hop peer.
telepresence-mcu-ts-directinterop	SIP trunks that directly interface with a TelePresence Server or MCU as the next hop peer.

# Add the Scripts

## Procedure

**Step 1** Download the scripts that you need from the Cisco website (go to relevant Unified CM software version and select **SIP Normalization and Transparency Scripts > Scripts**).

**Note** Skip this step if you are using Cisco Unified Communications Manager Version 10.5(2) or later, as the scripts are auto-installed with the software.

**Step 2** On Unified CM, go to **Device > Device Settings > SIP Normalization Script**.

**Step 3** Click **Add new**.

**Step 4** Click **Import File**.

**Step 5** Select the script that you downloaded.

**Step 6** Click **Import File**.

**Step 7** Enter or change the following details:

Name	Enter the script name. For example, telepresence-conductor-interop
Description	Enter a description. For example, Provides interoperability for calls through the TelePresence Conductor.
Memory Threshold	Enter 1000
Lua Instruction Threshold	Enter 2000

**Step 8** Click **Save**.

**Step 9** Repeat these steps until all the scripts you need are added.

**Step 10** To install the scripts onto the SIP trunks:

- On the Unified CM go to **Device > Trunk [or Media Resources] > Conference Bridge** for ad hoc conference bridges in Unified CM Version 9.1(2)SU2] and select the relevant trunk / bridge.
- In the Normalization script area of the SIP Information section, select the appropriate script for the trunk / bridge.
- Click **Save**.
- Click **Reset**.





## Migration Paths

---

- [Migration Overview, page 181](#)
- [Migration Prerequisites, page 182](#)
- [Supported Software Versions for Migration, page 182](#)
- [Migrate a Cisco Unified Communications Manager-only System to CMR Hybrid, page 183](#)
- [Separate Audio and Video Endpoints, page 183](#)
- [Migrate Cisco Unified Communications Manager and Cisco VCS to CMR Hybrid, page 184](#)
- [Comparison of Endpoint Capabilities, page 184](#)
- [Features and Version Dependencies, page 185](#)
- [Associated Products, Versions, and Features, page 185](#)

## Migration Overview

You can migrate previous solution deployments, to the preferred architecture. This release of CMR Hybrid uses the CMR Premises release 5.0 architecture which has two recommended deployment architectures for conferencing infrastructure:

- Conferencing infrastructure connected to Unified CM. This is the preferred architecture.
- Conferencing infrastructure connected to Cisco VCS.

For new (first-time) deployments the Unified CM-connected deployment should be implemented.

For existing audio and video deployments which do not match either of the two scenarios, we recommend that deployments are migrated to the CMR Premises 5.0 deployment using the 5.0 recommended code levels, as this is the tested architecture on top of which new feature developments are being planned.

To move to the CMR Hybrid deployment:

- Start by moving the infrastructure to the CMR Premises 5.0 standard.
- Then, if endpoints are currently registered to the Cisco VCS, move the endpoints that can register to Unified CM to Unified CM.

## Migration Prerequisites

CMR Premises release 5.0 makes use of endpoint caller IDs, displaying them in Roster lists and, if enabled, on-screen in conferences in TelePresence Server ActivePresence mode. We recommend reviewing the dial plan to ensure that displayed caller IDs are meaningful. For more information, see Provisioning Display Names Across the Solution in Provisioning Endpoint Display Names.

## Supported Software Versions for Migration

*Table 25: Supported Software Versions*

Product	Recommended	Minimum	Notes
TelePresence Server	4.2	4.1	TelePresence Server bridges must be configured for remote management by the TelePresence Conductor.
TelePresence Conductor	XC4.0	XC3.0 XC3.0.2 required for TSP audio	
MCU	4.5	4.5	
Cisco VCS	X8.5.3	X8.5	
Cisco VCS-for H.323 registration	X8.5.3	X8.5	
Cisco Expressway	X8.5.3	X8.5	
Cisco TMS	15.0	14.6	
Cisco TMSPE	1.5	1.4	
Unified CM	10.5(2)SU2	10.5(2)SU1	

# Migrate a Cisco Unified Communications Manager-only System to CMR Hybrid

## Procedure

- 
- Step 1** Upgrade Unified CM to the recommended version for CMR Hybrid.
  - Step 2** Add TelePresence Conductor to Unified CM and deploy bridges trunked to TelePresence Conductor; these components support all conference types.
  - Step 3** Upgrade endpoint software to the version supplied with Unified CM.
  - Step 4** Upgrade Cisco TMS/Cisco TMSPE to ensure support for Personal CMR / rendezvous and Scheduling.
  - Step 5** If WebEx participants are to be included in calls, ensure that Unified CM is running at least code version 9.1(2)SU2 and update Unified CM configuration to support Early Offer.
  - Step 6** To allow participants external to the company network to join conferences, deploy Cisco Expressway-C and Cisco Expressway-E for the firewall traversal.
  - Step 7** If Lync interop is required add a Cisco Expressway-C / Cisco VCS Control to be the gateway to the Microsoft Lync infrastructure. Version X8.5 or later is required. (See the Cisco VCS / Cisco Expressway deployment guides to identify whether Cisco VCS Control or Cisco Expressway-C is most appropriate for your needs.)
  - Step 8** If you want to add Legacy and H.323 endpoints to the solution, add a Cisco VCS Control onto which those endpoints can register.
- 

## Separate Audio and Video Endpoints

Some Unified CM deployments use a Unified CM for audio-only endpoints and a separate Unified CM for video endpoints. The ideal solution is to run both systems at the same Unified CM version, and in that case you should follow the [Migrate a Cisco Unified Communications Manager-only System to CMR Hybrid](#), on [page 183](#) instructions above.

If there are reasons why audio and video endpoints need to register to separate Unified CMs and they need to run different versions, then, before proceeding, verify with your account manager that the two Unified CM versions are acceptable in the deployment. In this case follow the [Migrate a Cisco Unified Communications Manager-only System to CMR Hybrid](#), on [page 183](#) instructions above on the video Unified CM.

# Migrate Cisco Unified Communications Manager and Cisco VCS to CMR Hybrid

## Procedure

- 
- Step 1** Upgrade Cisco VCS to the recommended version for CMR Hybrid.
- Step 2** Upgrade Unified CM to the recommended version for CMR Hybrid.
- Step 3** Move / keep TelePresence Conductor connected to Unified CM with bridges trunked to TelePresence Conductor.
- Step 4** If the TelePresence Conductor is moved from Cisco VCS, ensure that the search rules that used to send calls to the TelePresence Conductor under Cisco VCS now send the calls to Unified CM and that the Unified CM forwards these calls to TelePresence Conductor.
- Step 5** Cisco VCS architecture can remain as configured for firewall traversal, Lync interop and Legacy / H.323 endpoint registration.
- Step 6** Migrate endpoints that can register to Unified CM to Unified CM, upgrading software to the required versions for this solution release.
- 

## Comparison of Endpoint Capabilities

The following table compares the capabilities of endpoints registered to Unified CM and endpoints registered to Cisco VCS.

**Table 26: Endpoint Capabilities**

Capability	Registered to Unified CM	Registered to Cisco VCS
Phone books	TMS phone books Hierarchical directory	TMS phone books Hierarchical directory
Management	Managed by Unified CM & Prime Collaboration suite Provisioned by Unified CM	Managed by Cisco TMS Provisioned by Cisco TMS
Conference scheduling	Managed by Cisco TMS	Managed by Cisco TMS
Firewall traversal	Using Cisco Expressway-C and Cisco Expressway-E	Using Cisco VCS Expressway
Conference escalation	Ad hoc	Multiway

## Features and Version Dependencies

**Table 27: Features and Version Dependencies**

Feature	Versions Required
CMR provisioning and user portal	XC 3.0, TMS 14.6, TMSPE 1.4
TelePresence Server scalability improvements	TS 4.1
Basic TelePresence Server Cascade	TS 4.1, XC 3.0, TMSPE 1.4
TelePresence Server User Experience Improvements	TS 4.1
TelePresence Server Serviceability Improvements	TS 4.1
Single alias for host/guest conference, with role determined by PIN	TS 4.1, XC 3.0, TMS 14.6, TMSPE 1.4

## Associated Products, Versions, and Features

**Table 28: Associated Products, Versions, and Features**

Product	Versions	Features
MCU	4.5	<p>Minimum version for 4.0 operation. Adds:</p> <ul style="list-style-type: none"> <li>• ClearPath (Flux 1)</li> <li>• Separate content channel for encrypted SIP participants</li> <li>• Domain added for out dial requests without a domain—needed for WebEx out dial (for TSP conferenced audio) when the MCU is trunked to Unified CM.</li> </ul>
Unified CM	10.5(2)SU1	<p>Minimum version supported</p> <p>Ad hoc bridge now configured as data connection and explicit SIP trunk</p>
Cisco VCS	X8.5	Minimum version for Lync gateway operation in this release of CMR Hybrid
Cisco TMS	14.6	Minimum version for WebEx in CMR Hybrid and Host / Guest PIN

For more details about the CMR Premises solution and deployment, refer to the following guides:

- Cisco Collaboration Meeting Rooms (CMR) Premises Solutions Guide at <http://www.cisco.com/c/en/us/support/conferencing/collaboration-meeting-rooms-premises/model.html>
- Cisco Collaboration Meeting Rooms (CMR) Premises Deployment Guide at <http://www.cisco.com/c/en/us/support/conferencing/collaboration-meeting-rooms-premises/model.html>



# Set Up Cascading for Large-Scale or Critical Meetings

- [Cascading Overview, page 187](#)
- [Process for CMR Conferences, page 188](#)
- [Process for Scheduled Conferences, page 188](#)

## Cascading Overview

Within the local CMR Premises enterprise network, larger conferences that exceed the capacity of a single conference bridge can be cascaded (distributed) across one or more additional bridges. The bridges must be routable with each other and with Cisco TelePresence Conductor



### Note

Cascading is not supported from one conference bridge to another bridge that is outside the boundaries of the local enterprise network.

- Cascade links share only a single screen of video between TelePresence Server.
- Cascading is not supported from a TelePresence Server bridge to an MCU, or from an MCU to a TelePresence Server.
- On cascade-enabled conferences, cascading resources are reserved from the start of the conference for the configured Maximum number of cascades, whether or not they are actually used. For this reason we recommend using the cascade option sparingly—typically for large-scale meetings or for rendezvous conferences / personal CMRs used by VIP personnel.
- Cascading should not be enabled where certainty of resource availability is critical, such as the dedicated bridge scheduling case (where a single bridge in its own pool is reserved for scheduling).
- The ActiveControl feature on the TelePresence Server supports up to 500 participants.

## Process for CMR Conferences

This process uses the Cisco TMSPE provisioning extension of Cisco TMS to create a cascade-enabled CMR template and then apply it to a group. If your deployment does not use Cisco TMSPE, you can instead use the TelePresence Conductor to configure cascading, as described in the Conductor documentation.

### Procedure

- 
- Step 1** In Cisco TMS, go to **Systems > Provisioning > Users > Collaboration Meeting Room Templates** and create one or more templates as required.
  - Step 2** Check the **Allow Cascading** check box.
  - Step 3** Specify the maximum number of cascades allowed for a conference.
  - Step 4** In Cisco TMS, go to **Systems > Provisioning > Users**. Choose the relevant group, then select the button for the required template in the Active column.
- 

## Process for Scheduled Conferences

### Before You Begin

For deployments that use dedicated bridges for scheduling, cascading is not recommended (or possible in the case of a single pool with a single bridge). For deployments with shared-use bridges, which support both scheduled and non-scheduled conferences, the solution supports cascading of scheduled conferences on TelePresence Conductor-managed TelePresence Server or MCU conference bridges.

Cisco TMS will prompt you at booking time if the number of participants exceeds the single bridge capacity.

### Procedure

- 
- Step 1** **Book the scheduled conference as normal in Cisco TMS:** Add the TelePresence Conductor to the conference (unless if it defined as the default MCU).
  - Step 2** **Enable distribution for the conference:** In the settings for the conference created in the previous step, check the Distribution check box.
- 

### More Information

For details, see the Cisco TelePresence Conductor with Cisco TMS Deployment guide on the Cisco website at:

<http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html>