Cisco CMR Premises

Secondary Deployment Guide – Cisco VCS

First Published: April 2016

Last Updated: May 2016

Release 7.0

Cisco TelePresence Conductor XC4.2

Cisco TelePresence Management Suite 15.2

Cisco TMS Provisioning Extension 1.7

Cisco TelePresence Server 4.3

Cisco Systems, Inc. www.cisco.com

Contents

Preface

Change History

Table 1 Document Change History

Date	Changes	Reason
May 2016	Updated version.	Cisco TMS support for two-node TelePresence Conductor clusters is no longer a preview feature.
April 2016	First version.	New solution release.

About this Guide

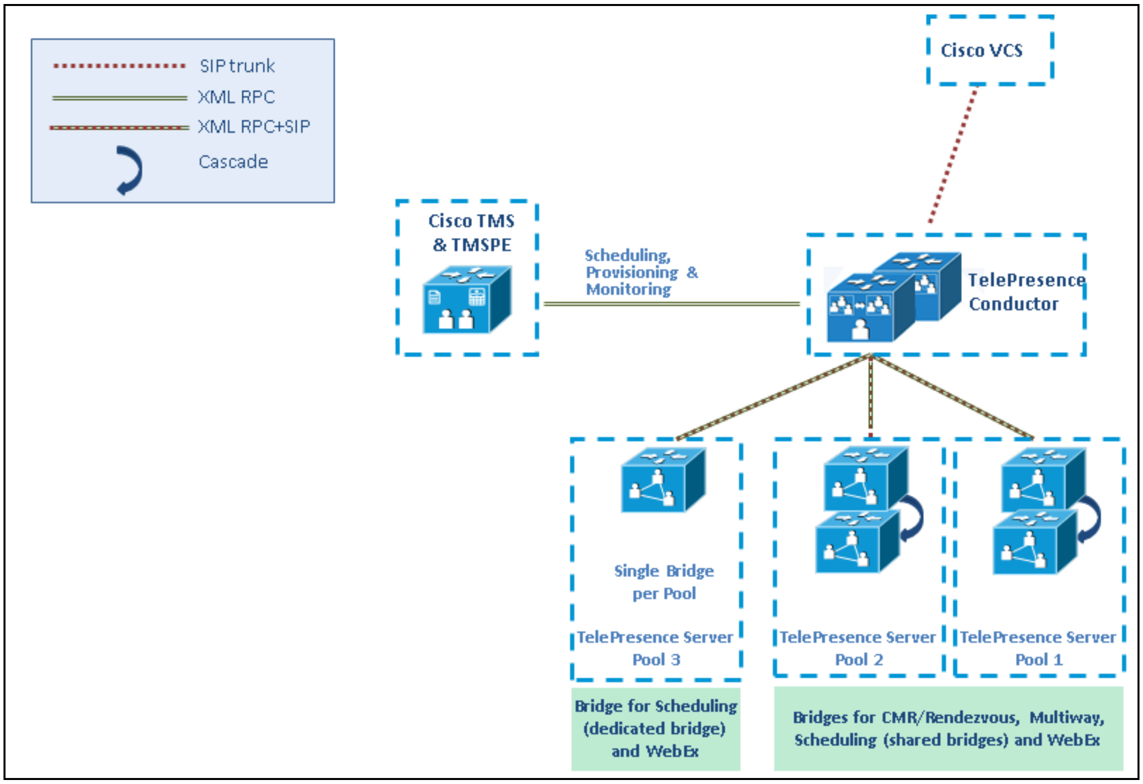
This guide describes how to implement the Cisco Collaboration Meeting Rooms (CMR) Premises solution across a video network. It summarizes the required processes and refers to the associated product guides for step-by-step details. For general information about the solution architecture and supported features see the accompanying *Cisco Collaboration Meeting Rooms (CMR) Premises Solution Guide*.

The guide and the product-related documents that it references are written for partners and technical sales people with a good technical understanding of Cisco video infrastructure products and their place in a video architecture. We assume that you are familiar with installing and configuring the relevant products.

This guide describes the secondary deployment for the solution, which uses the Cisco TelePresence Video Communication Server (Cisco VCS) for call control. If you use Cisco Unified Communications Manager for call control, refer instead to the primary deployment guide.

Solution Architecture Summary

Figure 1 High-level view of the architecture


SIP trunk
XML RPC
XML RPC+SIP
Cascade
Cisco VCS
Cisco TMS & TMSPE
Scheduling, Provisioning & Monitoring
TelePresence Conductor
Single Bridge per Pool
TelePresence Server Pool 3
TelePresence Server Pool 2
TelePresence Server Pool 1
Bridge for Scheduling (dedicated bridge) and WebEx
Bridges for CMR/Rendezvous, Multiway, Scheduling (shared bridges) and WebEx

Related Documentation

Title	Link
Cisco CMR Premises Deployment Guide - Secondary for Cisco VCS	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html
Cisco CMR Premises Solution Guide Release	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html
Cisco CMR Premises Release Notes	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-release-notes-list.html
Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html
Cisco TMS Provisioning Extension with Cisco VCS Deployment Guide	http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/products-installation-guides-list.html
Cisco TelePresence Conductor Administrator Guide	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-maintenance-guides-list.html
Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide	http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html
Cisco TelePresence Multiway™ Deployment Guide, Cisco VCS, MCU, Conductor	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html
Cisco Expressway Basic Configuration Deployment Guide	http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide	http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html
Cisco TelePresence Conductor with Cisco TMS Deployment Guide	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html
Cisco TMS Administrator Guide Version	http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html
Cisco CMR Hybrid Configuration Guide	http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-and-configuration-guides-list.html
Cisco TelePresence Conductor Product Programming Reference Guide	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-programming-reference-guides-list.html
Cisco Expressway Administrator Guide	http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html
Cisco VCS and Microsoft Lync Deployment Guide	http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

Title	Link
Cisco VCS Administrator Guide	http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-maintenance-guides-list.html

More Product Documentation on Cisco.com

Product	Link
TelePresence Conductor	http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/tsd-products-support-series-home.html
Cisco TMS	http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/tsd-products-support-series-home.html
Cisco TMSPE and Cisco TMSXE	http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html
TelePresence Server	http://www.cisco.com/c/en/us/support/conferencing/telepresence-server/tsd-products-support-series-home.html
MCU 5300 Series	http://www.cisco.com/c/en/us/support/conferencing/telepresence-mcu-5300-series/tsd-products-support-series-home.html
MCU MSE Series	http://www.cisco.com/c/en/us/support/conferencing/telepresence-mcu-mse-series/tsd-products-support-series-home.html
Cisco Expressway	http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html
Cisco VCS	http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/tsd-products-support-series-home.html
Unified CM	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Getting Started

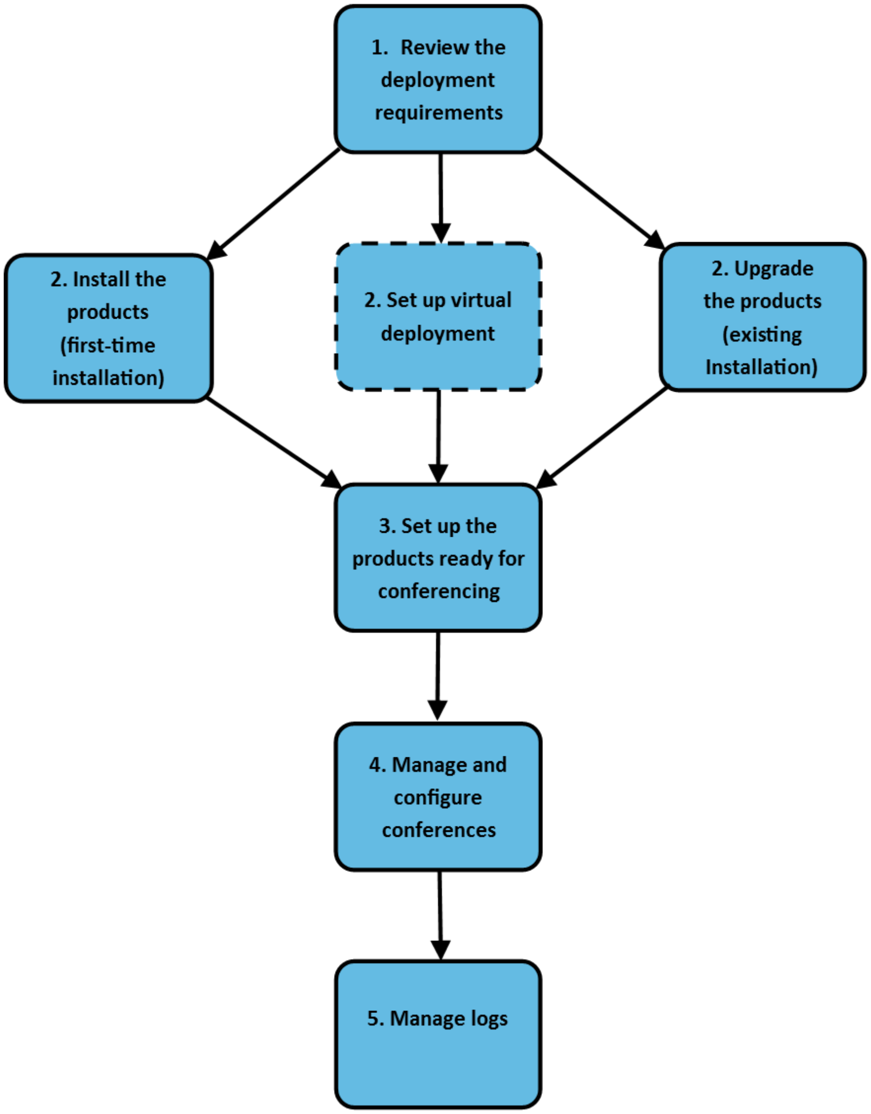

1. Review the deployment requirements
2. Install the products (first-time installation)
2. Set up virtual deployment
2. Upgrade the products (existing Installation)
3. Set up the products ready for conferencing
4. Manage and configure conferences
5. Manage logs

Figure 2 Sequence of tasks to set up and manage the solution

Deployment Requirements

Solution Products and Required Versions

To deploy the solution you need some or all of the products listed in this section, depending on which solution features you use. Each product you deploy must be running at a minimum the version specified here. The specified versions have been validated for this release of the solution.

Infrastructure Products

Note: Java 8 is required in this release of the solution.

Table 2 Infrastructure product versions validated for this release

Product	Version	Role
TelePresence Conductor	XC4.2	Conference resource allocation
Cisco TMS	15.2	Conference management & scheduling
Cisco TMSPE	1.7	Conference provisioning
Cisco TMSXE	5.2	[Optional] Conference scheduling for Microsoft environments
TelePresence Server	4.3*x* (latest)	Conference bridge resource
MCU 5300 Series, MCU MSE 8510	4.5*x* (latest)	Conference bridge resource
Cisco VCS Control In networks with multiple Cisco VCS installations, for full solution functions each one must be at the version specified here.	X8.7.1 X8.5.3 or X8.6 also acceptable. Except Microsoft Lync screen sharing needs X8.6. Clustering with Lync screen sharing needs X8.7.	Call control (Cisco VCS-Centric deployments). Microsoft Lync interworking. H.323 interworking.
Cisco VCS Expressway	X8.7.1 X8.5.3 or X8.6 also acceptable.	Secure firewall traversal. Registration of standards-based endpoints across the Internet.
Microsoft Windows Server	Windows Server 2012 SP2 64-bit Windows Server 2008 R2 64-bit also acceptable.	Database for Cisco TMS
Cisco WebEx	WBS30 or WBS31	Cloud conferencing with audio, video, and content sharing capabilities for WebEx clients

Microsoft Lync

If you want to support Microsoft Lync 2013 interoperability, you need Microsoft Lync Server 2013 and Lync 2013 for Windows clients. We do not support any other Lync servers or clients with the solution (including Skype for Business).

For more details about Lync 2013 server and client requirements, see:

- *Cisco Expressway and Microsoft Lync Deployment Guide* at Expressway Configuration Guides listing page, for Unified CM-based deployments.
- *Cisco VCS and Microsoft Lync Deployment Guide* at VCS Configuration Guides listing page, for VCS-based deployments.

Endpoints and Soft Clients

Table 3 Endpoint and soft client versions validated for this release

Product	Version
Cisco TelePresence MX200 G2, MX300 G2, MX700, MX800 (multistream-capable)	CE8.1 or TC7.3.6 CE software needed for enhanced layouts (multistream video).
Cisco TelePresence Quick Set SX20, SX80 (multistream-capable)	CE8.1 or TC7.3.6 CE software needed for enhanced layouts (multistream video).
Cisco TelePresence Quick Set SX10 (not multistream-capable)	CE8.1 or TC7.3.6
Cisco TelePresence EX Series EX60 and EX90	TC7.3.6
Cisco TelePresence Quick Set C20	
Cisco TelePresence Codec C Series C40, C60, C90	
Cisco TelePresence Profile Series	
Cisco TelePresence MX200 and MX300	
Cisco TelePresence TX9000 and TX9200 immersive systems	TX6.1.9

Configuration Requirements

Install Java 8

This release of the solution requires Java 8 to be installed.

Conference Bridges

The recommended 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 Conductor

TelePresence Conductor must be deployed using its back-to-back user agent (B2BUA). External policy server mode 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.

Reduce 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.

Setting the SIP TCP timeout value

- Version X8.6 and later. Do the following to set the SIP TCP timeout value:

  Go to **Configuration > Protocols > SIP** and set the value for **SIP TCP connect timeout**. For example, *1*

- Version X8.5.3. On version X8.5.3, the SIP TCP timeout value can't be configured through the web interface and instead you set it through the command line interface:

  1. Access the command line interface.
  2. Type this 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 control device, 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 (TLS is 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 Conductor **Location** and on the call controller (**Neighbor Zone**). See *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide* on the Conductor Configuration Guides page.

Media encryption from Cisco Expressway / Cisco VCS

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

1. Enable media encryption on the traversal client zone, from the Cisco Expressway-C / Cisco VCS Control toward 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.
2. Disable additional, unnecessary media encryption on the DNS egress zone, from the Cisco Expressway-E / Cisco VCS Expressway toward the Internet. To do this set **Media encryption mode** on that zone to *Auto*.

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.

- 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 under-subscription (see Task 8: Edit Service Preferences in Cisco TMS (optional), page 42).
  - 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, page 37 for more details.

Recommended Best Practices

Conference Bridges

- TelePresence Servers must be configured for remote management by Conductor (for 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. Compared to traditional screen licensing, Multiparty Licensing allows for greater capacity at lower cost. This deployment supports the Shared Multiparty licensing mode. With Shared Multiparty licensing, each license is shared by multiple users, but only in one conference at a time.

Note: Our recommended, primary deployment with Unified CM for call control supports Personal Multiparty licensing mode as well as Shared Multiparty.

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.

Resilience and Clustering

We recommend deploying the solution products in cluster configurations, for redundancy in case of a failure. Deploying clusters of TelePresence Conductors and multiple bridge pools ensures resilience for escalated and Personal CMR / rendezvous conferences. For future compatibility we recommend that TelePresence Conductor clusters are configured with no more than two nodes. If you currently deploy three-node clusters, you should consider removing a node. Cisco may discontinue the ability to add a third node to a cluster in a future software release.

Cisco TMS supports multiple TelePresence Conductors. You can configure TMS to fail over automatically from a primary Conductor node in a cluster to a subsidiary (peer) node if the primary node becomes unavailable. See Configuring TMS Support for Two-Node Conductor Clusters, page 54.

For details about Conductor clustering see *Cisco TelePresence Conductor Clustering with Cisco VCS (B2BUA) Deployment Guide* on the Conductor Configuration Guides listing page.

Content Channel

Most TelePresence endpoints support the use of a second video channel for content such as presentations.

- For MCU conference bridges, in the Conference template in TelePresence Conductor set **Content mode** to *Transcoded* (**Advanced parameters**). 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 Premises network is SIP-based. To connect H.323 endpoints to conferences within the CMR Premises network, the call must be interworked before it reaches the TelePresence Conductor. To do this configure the Cisco VCS Control 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 mode** to *On*. This interworks all incoming calls.

Escalated/Instant Conferencing

We do not support ad hoc conferencing (the Unified CM method of escalated conferencing) in the secondary deployment.

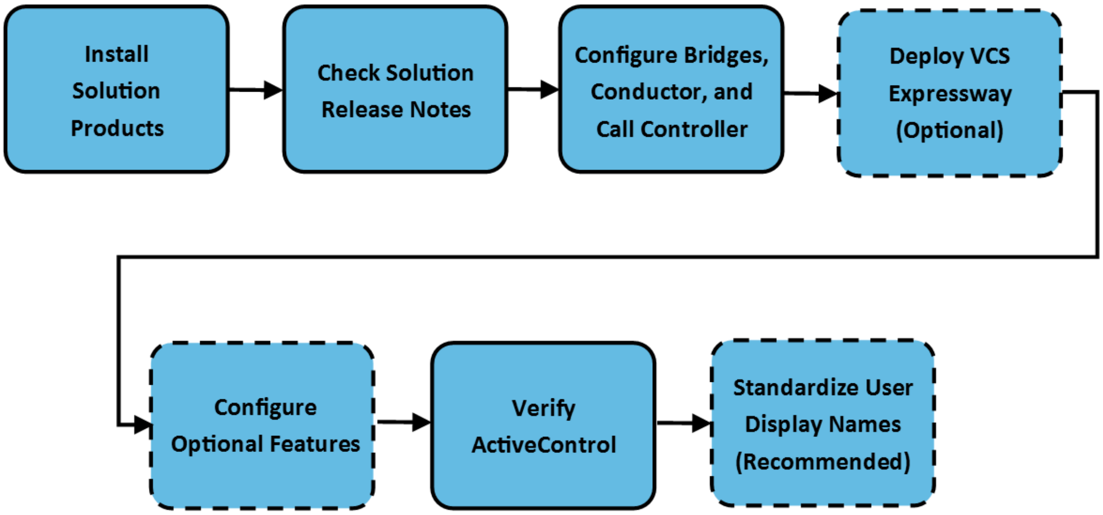
Microsoft Lync 2013 Interoperability

The solution supports interoperability with the Microsoft Lync 2013 service via interworking by the Cisco VCS Control (needs the *Microsoft Interoperability* key). For capacity reasons we recommend that you implement separate Cisco VCS Control devices for Lync access, and for other networking requirements respectively.

Installing the Solution Products - First-time Deployments

This section describes how to implement CMR Premises Release 7.0 as a first-time deployment. If you are upgrading from an earlier solution release, go to the Upgrading the Solution Products - Existing Deployments, page 24 instead.

Figure 3 Summary of first-time deployment tasks


Install Solution Products
Check Solution Release Notes
Configure Bridges, Conductor, and Call Controller
Deploy VCS Expressway (Optional)
Configure Optional Features
Verify ActiveControl
Standardize User Display Names (Recommended)

Before You Start

If you haven't already done so, review the Deployment Requirements, page 12.

You need a Cisco TelePresence Video Communication Server (Cisco VCS) for call control, already configured with a base configuration. See the Cisco VCS documentation on Cisco.com.

The other products to be installed for the solution depend on the features you use. As a minimum you will need:

- A TelePresence Conductor, configured according to its install guide and reachable via the network.
- One or more conference bridges, configured according to their install guide. We recommend TelePresence Servers, but MCUs are supported as an optional addition.
- Video endpoints.
- Cisco TelePresence Management Suite (Cisco TMS) is required if you want to schedule or monitor conferences.
- Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) is required if you want to use Personal CMRs.

If you use Multiparty Licensing with PMP licenses

If you use 4096-bit certificates on Conductor

To enable 4096-bit encryption on Cisco TMSPE, the following procedure must be followed for the Java software on Cisco TMSPE:

Edit **<jre-path>\lib\security\java.security** and insert an entry for bouncy castle as below (shown in **bold**). The other entries are incremented by 1, so the contents should be:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider
security.provider.6=com.sun.crypto.provider.SunJCE
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.10=sun.security.smartcardio.SunPCSC
security.provider.11=sun.security.mscapi.SunMSCAPI
```

Note: If you do not make the above change, TMSPE cannot access Conductor and users will not be able to edit their Personal Collaboration Meeting Rooms (CMRs). In addition, the following error is displayed in the TMSPE logs: *VMR::ConductorConnector - TelePresence Conductor failure with: Could not generate DH keypair*.

Task 1: Install the Solution Products

Install each product that you need for your solution deployment at the required version for 7.0. We recommend that you install the products in the order listed here.

Table 4 Order to upgrade / install the products

Order	Product	Version	Install guide	Software download
1	Cisco VCS (if not already installed)	X8.7.1 X8.5.3 or X8.6 also acceptable. Except Microsoft Lync screen sharing needs X8.6. Clustering with Lync screen sharing needs X8.7.	X8.7 Installation Guide for your VCS platform	VCS
2	Cisco VCS Expressway, if used	X8.7.1 X8.5.3 or X8.6 also acceptable.	X8.7 Installation Guide for your Expressway platform	VCS
3	Cisco TMS	15.2	TMS Installation and Upgrade Guide 15.0	TMS
4	Upgrade/ set up endpoints	See Solution Products and Required Versions, page 13. Endpoints must be registered to Cisco VCS.		

Table 4 Order to upgrade / install the products (continued)

Order	Product	Version	Install guide	Software download
5	Cisco MCU, if used	4.5.*x* (latest)	■ MCU 5300 Series Install Guide ■ MCU MSE 8510 Installation Guide	MCU
6	TelePresence Server	4.3.*x* (latest)	■ Cisco TelePresence Server on Multiparty Media 820 Installation Guide ■ Cisco TelePresence Server 7010 Installation Guide ■ TelePresence Server MSE 8710 Installation Guide ■ TelePresence Server on Virtual Machine Installation Guide ■ TelePresence Server on Multiparty Media 310/320 Installation Guide	TelePresence Server
7	Cisco TMSPE	1.7 Install Java 8 before Cisco TMSPE	Cisco TMSPE Deployment Guide	TMSPE
8	TelePresence Conductor	XC4.2	Cisco TelePresence Conductor Virtual Machine Installation Guide	Conductor
9	Cisco TMSXE, if used	5.2	Cisco TMSXE Deployment Guide	TMSXE

Task 2: Check Solution Release Notes

Check for any configuration requirements in the latest solution *Release Notes* for Release 7.0 on the CMR Premises solution documentation page and action any necessary steps.

Task 3: Configure Conference Bridges, Conductor, and Call Control Device

Connect TelePresence Conductor to the conference bridges and Cisco VCS, and configure for CMR Premises. See Connecting TelePresence Conductor, page 28 for instructions.

Task 4: Deploy Cisco VCS Expressway for Remote Access (Optional)

If you need participants outside of the company network to participate in the video conferences, deploy Cisco VCS Expressway for the firewall traversal (if not already in place).

Task 5: Configure Cisco VCS for Microsoft Lync (Optional)

If you need interoperability with Microsoft Lync, follow the instructions to configure Cisco VCS in the latest *Cisco VCS and Microsoft Lync Deployment Guide X8.7* at VCS Configuration Guides page.

Task 6: Configure TMS for Conductor Failover

This task applies if you use clustered Conductors. You can configure Cisco TMS to automatically transfer to a peer Conductor node if the primary Conductor fails. See Configuring TMS Support for Two-Node Conductor Clusters, page 54 for instructions.

Task 7: Set Up CMR Hybrid for WebEx Participation (Optional)

If you need to set up an integration with the CMR Hybrid service, see Using CMR Hybrid in Scheduled Conferences, page 55 for instructions. After you set up the integration, you can optionally add WebEx meetings to Personal CMRs (see Using CMR Hybrid with Personal CMRs, page 57).

Task 8: Verify ActiveControl and IX Protocol Configuration

1. Check that the iX protocol is configured correctly in the relevant solution components, as described in Using ActiveControl, page 69. The iX protocol is a prerequisite for ActiveControl to endpoints.
2. This step applies if your CMR Premises network connects to Unified CM systems that run Version 8.*x* or earlier, or to third-party networks. In such cases, to avoid unpredictable results you should disable the iX protocol on all relevant trunks. This isolates iX traffic from external systems that do not support it. See Limiting ActiveControl in External Connections, page 70 for instructions.

Note: The iX protocol is also a prerequisite for multistreaming video to endpoints, for enhanced layouts support.

Task 9: Standardize User Display Names

To ensure that the participant names displayed in conferences are consistent across the solution, we recommend following the configuration steps in Appendix 1: Provisioning Display Names Across the Solution, page 77.

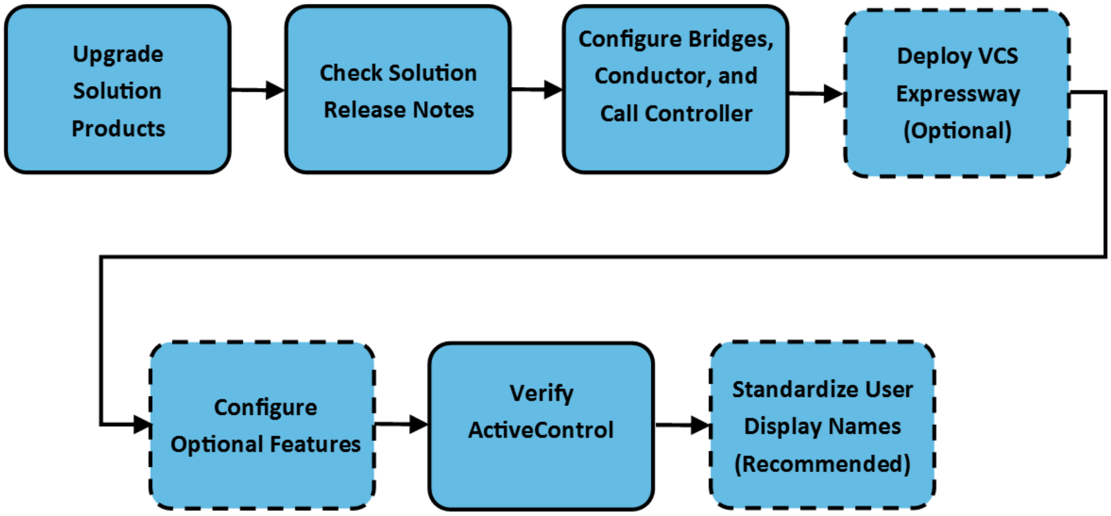
What Next?

Now go to the section Setting Up the Solution Products Ready for Conferencing, page 1.

Upgrading the Solution Products - Existing Deployments

This section describes how to upgrade an existing deployment to Release 7.0. If you are installing CMR Premises for the first time, go to the Installing the Solution Products - First-time Deployments, page 20 instead.

Figure 4 Summary of deployment upgrade tasks


Upgrade Solution Products
Check Solution Release Notes
Configure Bridges, Conductor, and Call Controller
Deploy VCS Expressway (Optional)
Configure Optional Features
Verify ActiveControl
Standardize User Display Names (Recommended)

Before You Start

If you haven't already done so, review the Deployment Requirements, page 12.

If you use endpoints running CE software

If your CE endpoints are running CE8.1 software (recommended), you must also update your Cisco TMS software to Version 15.1 or later (15.2 is recommended for this release).

If you use Multiparty Licensing with PMP licenses

If you use 4096-bit certificates on Conductor

To enable 4096-bit encryption on Cisco TMSPE, the following procedure must be followed for the Java software on Cisco TMSPE:

Edit **<jre-path>\lib\security\java.security** and insert an entry for bouncy castle as below (shown in **bold**). The other entries are incremented by 1, so the contents should be:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=sun.security.ec.SunEC

security.provider.5=com.sun.net.ssl.internal.ssl.Provider

security.provider.6=com.sun.crypto.provider.SunJCE

security.provider.7=sun.security.jgss.SunProvider

security.provider.8=com.sun.security.sasl.Provider

security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI

security.provider.10=sun.security.smartcardio.SunPCSC

security.provider.11=sun.security.mscapi.SunMSCAPI
```

Note: If you do not make the above change, TMSPE cannot access Conductor and users will not be able to edit their Personal Collaboration Meeting Rooms (CMRs). In addition, the following error is displayed in the TMSPE logs: *VMR::ConductorConnector - TelePresence Conductor failure with: Could not generate DH keypair*.

Virtual Conference Bridges

The Cisco TelePresence Server on Virtual Machine has been migrated to a new platform in this release. You must **redeploy** any Cisco TelePresence Server on Virtual Machines with the new OVA file, as it's not possible to migrate the platform via a software upgrade.

A script to support the migration process is available from the TelePresence Server software download page on Cisco.com. The script ensures that your existing bridge configurations, keys, and serial numbers are preserved. Detailed instructions are available on the TelePresence Server Install and Upgrade Guides page.

Task 1: Upgrade the Solution Products

Upgrade each product in your solution deployment to the versions specified in the table below. We recommend that you upgrade the products in the order listed here.

At this stage, do *not* update your configuration for 7.0 functionality.

Table 5 Order to upgrade / install the products

Order	Product	Version	Install guide	Software download
1	Cisco VCS (if not already installed)	X8.7.1 X8.5.3 or X8.6 also acceptable. Except Microsoft Lync screen sharing needs X8.6. Clustering with Lync screen sharing needs X8.7.	X8.7 Installation Guide for your VCS platform	VCS
2	Cisco VCS Expressway, if used	X8.7.1 X8.5.3 or X8.6 also acceptable.	X8.7 Installation Guide for your Expressway platform	VCS
3	Cisco TMS	15.2	TMS Installation and Upgrade Guide 15.0	TMS
4	Upgrade/ set up endpoints	See Solution Products and Required Versions, page 13. Endpoints must be registered to Cisco VCS.		
5	Cisco MCU, if used	4.5.*x* (latest)	■ MCU 5300 Series Install Guide ■ MCU MSE 8510 Installation Guide	MCU

Table 5 Order to upgrade / install the products (continued)

Order	Product	Version	Install guide	Software download
6	TelePresence Server	4.3.*x* (latest)	- Cisco TelePresence Server on Multiparty Media 820 Installation Guide - Cisco TelePresence Server 7010 Installation Guide - TelePresence Server MSE 8710 Installation Guide - TelePresence Server on Virtual Machine Installation Guide - TelePresence Server on Multiparty Media 310/320 Installation Guide	TelePresence Server
7	Cisco TMSPE	1.7 Install Java 8 before Cisco TMSPE	Cisco TMSPE Deployment Guide	TMSPE
8	TelePresence Conductor	XC4.2	Cisco TelePresence Conductor Virtual Machine Installation Guide	Conductor
9	Cisco TMSXE, if used	5.2	Cisco TMSXE Deployment Guide	TMSXE

Task 2: Verify New Versions in Existing Configuration

Verify that the new software runs satisfactorily on your existing solution configuration and that the network is functioning as you expect.

Task 3: Check Solution Release Notes

Check for any configuration requirements in the latest solution *Release Notes* for Release 7.0 on the CMR Premises solution documentation page and action any necessary steps.

Task 4: Configure Conference Bridges, Conductor, and Call Control Device

Connect TelePresence Conductor to the conference bridges and Cisco VCS, and configure for CMR Premises. See Connecting TelePresence Conductor, page 28 for instructions.

Task 5: Deploy Cisco VCS Expressway for Remote Access (Optional)

If you need participants outside of the company network to participate in the video conferences, deploy Cisco VCS Expressway for the firewall traversal (if not already in place).

Task 6: Configure Cisco VCS for Microsoft Lync (Optional)

If you need interoperability with Microsoft Lync, follow the instructions to configure Cisco VCS in the latest *Cisco VCS and Microsoft Lync Deployment Guide X8.7* at VCS Configuration Guides page.

Task 7: Configure TMS for Conductor Failover

This task applies if you use clustered Conductors. You can configure Cisco TMS to automatically transfer to a peer Conductor node if the primary Conductor fails. See Configuring TMS Support for Two-Node Conductor Clusters, page 54 for instructions.

Task 8: Set Up CMR Hybrid for WebEx Participation (Optional)

If you need to set up an integration with the CMR Hybrid service, see Using CMR Hybrid in Scheduled Conferences, page 55 for instructions. After you set up the integration, you can optionally add WebEx meetings to Personal CMRs (see Using CMR Hybrid with Personal CMRs, page 57).

Task 9: Verify ActiveControl and IX Protocol Configuration

1. Check that the iX protocol is configured correctly in the relevant solution components, as described in Using ActiveControl, page 69. The iX protocol is a prerequisite for ActiveControl to endpoints.
2. This step applies if your CMR Premises network connects to Unified CM systems that run Version 8.*x* or earlier, or to third-party networks. In such cases, to avoid unpredictable results you should disable the iX protocol on all relevant trunks. This isolates iX traffic from external systems that do not support it. See Limiting ActiveControl in External Connections, page 70 for instructions.

Note: The iX protocol is also a prerequisite for multistreaming video to endpoints, for enhanced layouts support.

Task 10: Standardize User Display Names

To ensure that the participant names displayed in conferences are consistent across the solution, we recommend following the configuration steps in Appendix 1: Provisioning Display Names Across the Solution, page 77.

What Next?

Now go to the section Setting Up the Solution Products Ready for Conferencing, page 1.

Connecting TelePresence Conductor

This topic explains how to connect Conductor to the bridges and to Cisco VCS.

Before You Start

- Conductor must be installed according to the instructions in Cisco TelePresence Conductor Getting Started or Cisco TelePresence Conductor Virtual Machine Installation Guide.
- Cisco VCS must be installed and configured to act as a SIP registrar and proxy. Ensure connectivity by registering at least three endpoints. Then check that they can all call each other with voice and video.
- One or more bridges must be powered on and accessible to Conductor over HTTP/HTTPS and SIP TLS. HTTPS is recommended in all cases and is required for Multiparty Licensing to work.

Task 1: Configure Conductor for CMR Premises

Follow the step-by-step instructions in *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide* on the Conductor Configuration Guides page. These instructions explain how to:

- Design a dial plan to define the aliases and call routes in your network.
- Configure the TelePresence Server.
- Configure the Cisco TelePresence MCU Series.
- Configure Cisco VCS with a neighbor zone and search rule for Conductor.
- Configure Conductor in B2BUA mode (using the Cisco VCS external policy service is not supported).

Important The following caveat applies: Set the VCS **Zone profile** for the trunk between Cisco VCS Control and Conductor to *Custom* and set **Automatically respond to SIP searches** to *On*. For details, see *Adding the TelePresence Conductor as a neighbor zone* in the *Cisco TelePresence Conductor with Cisco TelePresence VCS (B2BUA) Deployment Guide*.

When the steps in the *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide* are complete, you have the following elements set up:

- A SIP trunk between Cisco VCS Control and Conductor.
- A Location in Conductor for the trunk (with or without a dial-out address). Depending on your requirements you may define multiple Locations.
- A neighbor zone in VCS for the trunk.
- Configured bridge resources.

Task 2: Enable Multiparty Licensing (Recommended)

1. Log in to Conductor.
2. Ensure there are no active calls on Conductor. Any currently active calls are ended when you enable Multiparty Licensing.
3. Go to **Maintenance > Option key**.

4. Under **Software option** in the **Add option key** field, enter the option key for the Shared Multiparty (SMP) licenses you have purchased.
5. Click **Add option**.
6. Repeat for any other SMP license keys you have purchased. License keys are additive, so for example, two option keys for 100 SMP licenses result in 200 licenses.
7. On the same page, under **Multiparty Licensing**, set **Multiparty licensing for TelePresence Servers** to *Enabled*.
8. You can now apply the Multiparty licenses to end users, as described in Managing Multiparty Licensing, page 51.

Task 3: Enable Personal CMR / rendezvous Conferences

Note: The preferred approach for permanent conferencing is to deploy Personal CMRs rather than rendezvous conferences.

1. To deploy Personal CMRs, follow the instructions described in About Personal CMRs, page 45.
2. If you use Multiparty Licensing, note that no further configuration is required to support them for Personal CMR conferencing.
3. If you need rendezvous conferences, you manually configure them directly on Conductor, as follows:
   a. Go to **Conference configuration > Conference aliases** and create an alias for rendezvous conferencing.
   b. Then on the Cisco VCS, define a search rule to point to the appropriate zone
4. Personal CMR / rendezvous conferences rely on the dialed number/URI to determine the bridge used. Appropriate configuration is needed in Conductor and Cisco VCS to ensure that the correct bridges are selected.

More detail is available in *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide on the Conductor Configuration Guides page*.

Task 4: Enable Scheduled Conferences

1. You need to create dedicated conference templates and conference aliases on Conductor, so that Cisco TMS can schedule against them. See How to Enable Scheduled Conferencing, page 40.
2. Personal CMRs cannot be scheduled through Cisco TMS. (The Personal CMR details can of course be added to an invite for the participant to dial into the CMR.)

Assuming that Conductor and Cisco VCS are configured as described above, scheduled conferences rely on the dialed number/URI to determine the bridge used.

Task 5: Enable Multiway Conferences

Multiway conferencing provides instant/escalated conferences. Cisco VCS routes Multiway requests direct to Conductor. The Multiway conference is hosted on a Conductor-managed bridge. If you want to support Multiway conferences, complete these tasks to route Multiway calls through the Cisco VCS Control:

1. To optionally use Cisco TMS to provision endpoints with unique Multiway URIs, you need the Cisco VCS device provisioning option key installed. The supported method is to use Cisco TMSPE with a Cisco VCS running in Provisioning Extension mode.
2. If you use a dedicated number range for Multiway, define a search rule in the Cisco VCS to route the Multiway aliases to the Conductor neighbor zone.
3. Optionally configure a dedicated Multiway conference alias on Conductor.
4. Configure Multiway on the relevant endpoints. You can do this manually or using Cisco TMSPE.

What Next?

CMR Premises is now installed on all the solution products, with each conferencing method enabled. The rest of this guide describes how to do any of the following tasks, depending on your local requirements:

- Managing Personal CMRs.
- Managing scheduled conferences.
- Configuring conference services, like cascading.
- Configuring conference features, like Active Meeting Manager.

Virtual Deployments on Cisco Business Edition 6000 / 7000

You can deploy the solution as a virtualized application on the Cisco Business Edition 6000 (BE6000) or Cisco Business Edition 7000 (BE7000) platforms.

Hardware and Sizing

The standard sizing and hardware guidelines for all Cisco Unified Communications (UC) applications on Unified CM deployments apply:

- http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Sizing_Guidelines
- http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware

Physical CPU cores must not be over-subscribed for UC virtual machines. One physical CPU core must equal one virtual machine vCPU core.

You should enable hyperthreading on the CPU when available. But note the resulting logical cores do not change standard UC app rules. The rules use one-to-one mapping of physical cores-to-vCPU, not logical cores-to-vCPU.

Details about running UC applications in a virtualized environment are available in http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment

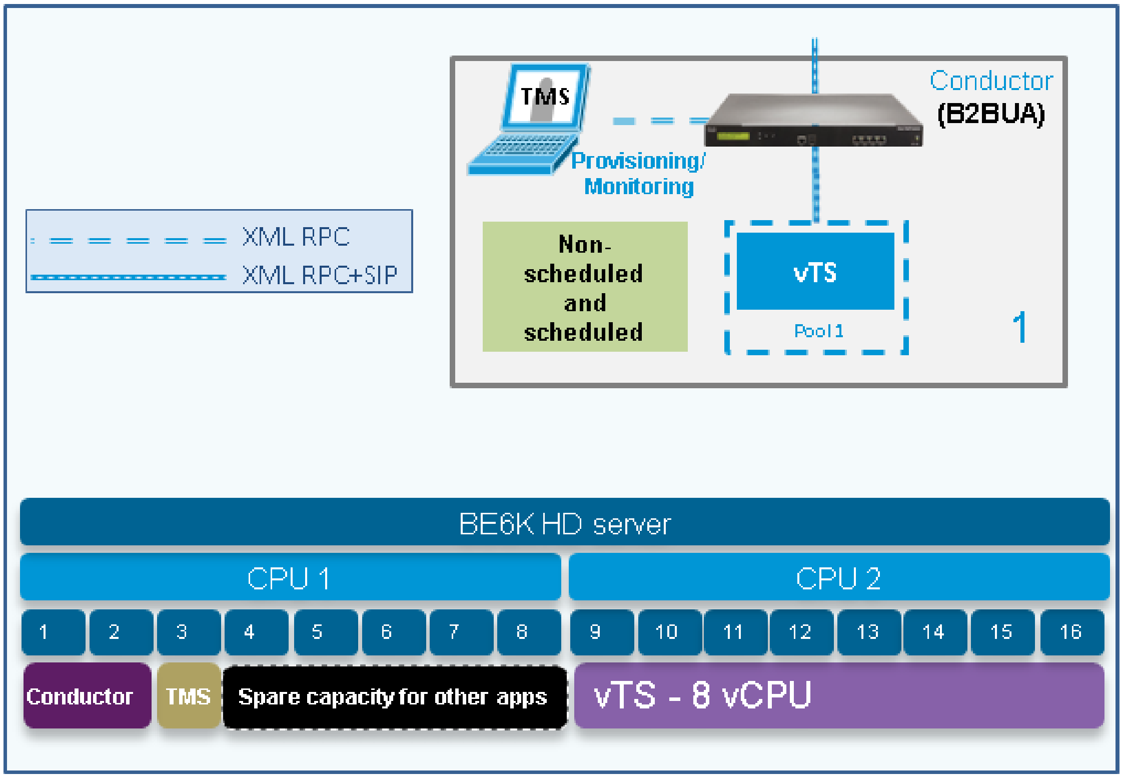
The Virtual Machine Placement Tool on Cisco.com is available to assist with planning VM-to-physical server placement. You can use it to quickly check what virtual machine configuration is appropriate for a given physical server configuration.

Recommended Configuration

Many BE6000/BE7000 configurations are compatible with CMR Premises. The following configuration is the one that we test for the solution. All elements must be running the required versions for CMR Premises (Solution Products and Required Versions, page 13):

- BE6000 Product ID BE6K-SW-9X10X-XU or BE7000 Product ID BE7K-SW-9X10X-XU
- Cisco Business Edition 6000/7000 High Density or Cisco Business Edition 7000 Medium Density server (they have two 8-core CPUs).
- Hyperthreading enabled.
- One-core virtualized Cisco TMS.
- Two-core virtualized Cisco TelePresence Conductor (Select version).
- Eight-core Cisco TelePresence Server on Virtual Machine conference bridge.
- Optionally a physical Cisco Expressway for remote user access.
- Cisco VCS for call control. You can run the call control on the remaining cores or on another BE6000/BE7000 unit.

Figure 5 Solution on BE6000/BE7000 (using a shared bridge for scheduled and non-scheduled conferences)



Scaling Up

This deployment can be scaled up by running additional vTS instances on further BE6000/BE7000 systems or by adding dedicated hardware. Depending on their capacity requirements, scaled-up deployments may need either Conductor Select or full capacity Conductor licenses.

Using a Dedicated Bridge for Scheduled Conferences

The default BE6000 and BE7000 configurations support only a single Cisco TelePresence Server on Virtual Machine (vTS) conference bridge. This has implications if you want to use a dedicated bridge for scheduled conferences. In this case the sole bridge will be available only for scheduled conferences. If you also want to support non-scheduled conferences (Personal CMR / rendezvous, Multiway) you need to use additional TelePresence Servers. The additional units can be virtual machines or physical appliances.

Managing Scheduled Conferencing

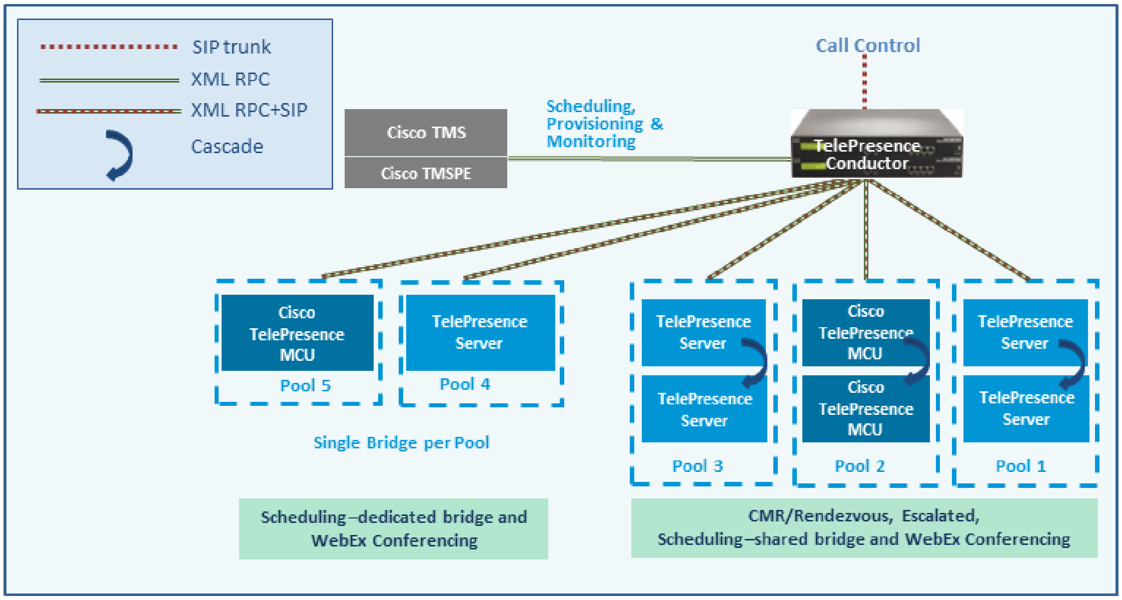
How Scheduling Works in the Solution

The solution supports two scheduling methods:

- Shared bridge. Our recommended method is to allow bridges to be shared for non-scheduled as well as scheduled conferences.
- Dedicated bridge. Alternatively you can deploy one or more bridges that are reserved just for scheduled conferences. Each bridge is in a pool of its own, with or without a second dedicated bridge-and-pool combination for backup.

Note: With shared bridges, although the system will reserve the correct meeting resources based on the booking, it is possible for those resources to be over-subscribed for the meeting. For example if unexpected participants or unscheduled rooms join the conference. Also, resources may be used up by non-scheduled conferences, without Cisco TMS being aware of it.

Figure 6 Scheduling configurations



TelePresence Conductor and Cisco TMS Interaction

Setting up scheduling involves configuration tasks on both the TelePresence Conductor and on Cisco TMS. The TelePresence Conductor configuration determines what conference resource information is passed to Cisco TMS. The configuration for Cisco TMS determines how that information is used (such as conference priority and participant numbers).

Alias pattern matching

Scheduling is coordinated between the TelePresence Conductor and Cisco TMS through alias pattern matching. The **Alias Pattern** setting in the Cisco TMS alias must match the **Incoming alias** setting in the conference alias in TelePresence Conductor (and the corresponding pattern on the call control device).

Cisco TMS sends its alias pattern to the TelePresence Conductor, which checks for a matching pattern in its conference aliases. When TelePresence Conductor finds a match, it returns to Cisco TMS the Service Preference settings and other relevant information associated with the matching conference alias.

Multiple conference aliases can share the same Service Preference.

Service Preference and conference priority

The Service Preference on TelePresence Conductor is a key element in managing scheduling. Bridge resources can optionally be reserved for scheduled conferences only (the dedicated bridge case). To do this:

1. " Mark" the relevant conference bridge pools in the TelePresence Conductor Service Preference (**Pools to use for scheduling** option). Conductor only notifies TMS about the pools that are marked for scheduling.
2. Make sure that the relevant pool is only used in a single Service Preference, which is not used for non-scheduled conferencing.
3. Set **Scheduled conference** in the TelePresence Conductor template to *Yes*.

Managing the priority of Cisco TMS conference aliases (optional)

Cisco TMS assigns a conference alias automatically when it creates a conference. Optionally you can change the variable part during booking, per individual conference. Cisco TMS first tries to use the alias that has the lowest priority number assigned to it (the lower the priority number the *higher* the priority). If the capacity of that Service Preference on Cisco TMS is used up, Cisco TMS selects the alias with the next lowest priority number on another Service Preference, and so on.

Modeling tool

A Resource Cost Calculator tool is available in Cisco TMS from **Systems > Navigator > Conductor > Service Preferences**. This can be helpful in planning your configuration.

IP Zones in Cisco TMS

Only the IP Zone of the TelePresence Conductor itself is relevant to Cisco TMS bookings, since TelePresence Conductor is the entity that is scheduled. Individual IP Zones for different pools, Service Preferences, or conference aliases in the TelePresence Conductor are not configured in Cisco TMS.

Conference Bridges in Cisco TMS

You can if you wish add TelePresence Conductor-managed conference bridges to Cisco TMS (the bridges are automatically defined as non-bookable in Cisco TMS). This gives the following advantages:

- Conference snapshots in the Cisco TMS **Conference Control Center** are available for Cisco TelePresence MCU bridges.
- Some reporting functionality. Calls are reported in Call Detail Records, but not tied to Cisco TMS conferences.
- Health monitoring for the bridges.

Multiparty Licensing

Cisco TMS has no information about the number of Multiparty licenses that are available on a particular TelePresence Conductor. You need to monitor the alarms on TelePresence Conductor and tickets on Cisco TMS to check that you are not exceeding the valid number of licenses.

More Information

- *Cisco TelePresence Management Suite Administrator Guide*
- *Cisco TelePresence Conductor Administrator Guide*
- *Cisco TelePresence Conductor API Guide*
- *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide*
- *Cisco TelePresence Conductor with Cisco TMS Deployment Guide*

Limitations and Requirements for Scheduled Conferencing

Limitations

Caution: If you use clustered TelePresence Conductors, be aware that for failover purposes, 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).

Users cannot schedule meetings to their Personal CMRs via the Cisco TMSPE user portal. However, when they schedule meetings through Microsoft Outlook, users can include their Personal CMR for the meeting simply by adding the CMR alias to the “Location” field in the meeting invite.

If you deploy the CMR Hybrid service, and have TSP Audio from a TSP that uses the same bridge as the previous scheduled conference, we recommend you turn off the auto-extend function in TMS.

TelePresence Conductor may wait up to 30 seconds before releasing resources between meetings. This may cause denial of inbound and outbound calls for back-to-back meetings, and utilization spikes if participants repeatedly leave and join a meeting.

Requirements

- Ensure that the solution-level prerequisites and configuration process for CMR Premises are complete.
- The solution requires the Cisco TMS management tool for scheduling. Conferences are not scheduled directly on TelePresence Conductor.
- Participants in a scheduled conference should not escalate to a Multiway (instant/escalated) conference. This causes a degraded conference experience for participants.
- If you use dedicated conference bridges for scheduling, some additional points apply, as described in the next section.

Requirements for Dedicated Bridge Scheduling

- The bridge resources will only be used for scheduled conferencing (subject to correct configuration). TelePresence Conductor supplies Cisco TMS with a list of just the 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, the optimization will reduce the capacity needed on the shared backup bridge(s).

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 instant/escalated 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.

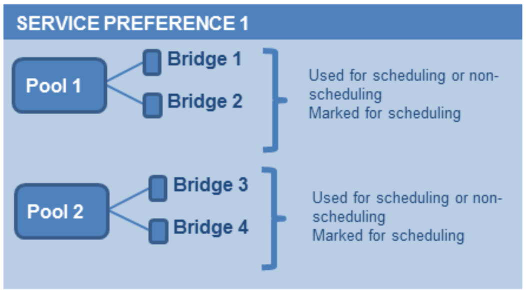
Shared Bridges

This is the recommended shared-bridge approach, which allows other types of conferences as well as scheduled conferences to run on the conference bridges:

Table 6 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 non-scheduled conferences. All pools are marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS. We recommend enabling cascading in this scenario, otherwise conferences may fail in some circumstances.	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 under-allocate capacity below 100%. Only the specified reduced percentage is made available to TMS for scheduling conferences, rather than the actual capacity.

Example 1 – shared use



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:

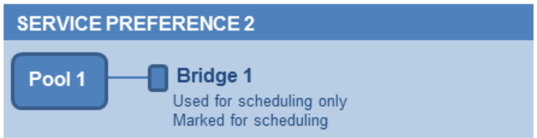
Table 7 Deploying dedicated bridge(s) for scheduling

	Service Preference contains ...	Configuration	Advantages	Disadvantages
Example 2	Dedicated bridge for scheduled conferences.	Single pool, with a single conference bridge. Pool marked to be used for scheduling in the TelePresence Conductor Service Preference. Pool is reported to Cisco TMS in capacity information requests.	Conference availability is guaranteed, subject to bridge failure (or full capacity). Maximizes use of resources, as Cisco TMS will book ports until the bridge is full.	Uses one conference bridge exclusively for scheduling. Cascaded conferencing does not occur: to avoid wasting resources, cascading should be disabled.
Example 3	- Dedicated bridge for scheduled conferences - Dedicated backup bridge	Two pools. Both pools contain a single conference bridge. The second pool is used as a backup if the bridge in the highest priority pool fails. Only the first pool is marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.	As for Example 2, with added benefit of fallback in case of bridge failure.	Uses two conference bridges exclusively for scheduling. Consumes backup resources. To avoid wasting resources, cascading should be disabled.
Example 4	- Dedicated bridge for scheduled conferences - Shared-use backup bridges for both scheduled and non-scheduled conferences	Two or more pools. Highest priority pool with one bridge only, used for scheduled conferences. Other pools contain bridges for both scheduled (as backup) and non-scheduled conferences. Only the first pool is marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.	As for Example 2, with possible benefit of fallback in case of bridge failure if the other pools have spare capacity.	Uses one conference bridge exclusively for scheduling. To avoid wasting resources on the dedicated bridge, cascading should be disabled.

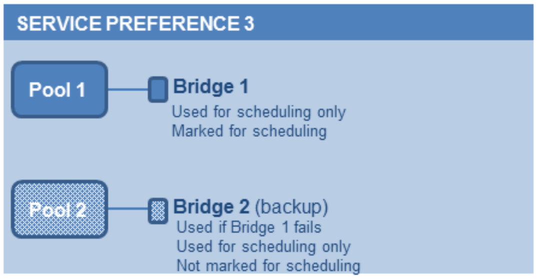
Table 7 Deploying dedicated bridge(s) for scheduling (continued)

	Service Preference contains ...	Configuration	Advantages	Disadvantages
Example 5	▪ Dedicated bridges for scheduled conferences ▪ Shared-use backup bridges for both scheduled and non-scheduled conferences	Two or more pools. Highest priority pool with two or more bridges, used for scheduled conferences. Cascading enabled on the associated conference template. Other pools contain bridges for both scheduled (as backup and overflow) and non-scheduled conferences. Only the first pool is marked for scheduling in the TelePresence Conductor Service Preference and reported to Cisco TMS.	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. Bridges in the backup pools are used for scheduling if: ▪ A bridge in Pool 1 fails. ▪ Cascading in Pool 1 uses up bridge resources that Cisco TMS expected to be available for scheduling.	Uses conference bridges exclusively for scheduling. If scheduled conferences are cascaded, they may need resources from a shared-use pool.

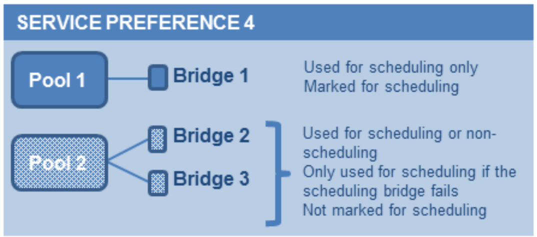
Example 2



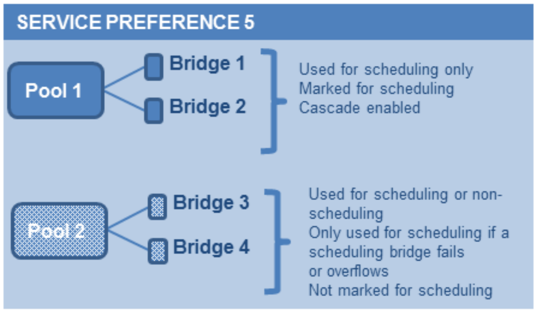
Example 3



Example 4


SERVICE PREFERENCE 4
Pool 1
Bridge 1
Used for scheduling only
Marked for scheduling
Pool 2
Bridge 2
Bridge 3
Used for scheduling or non-scheduling
Only used for scheduling if the scheduling bridge fails
Not marked for scheduling

Example 5



How to Enable Scheduled Conferencing

Before You Start

- Check that the tasks in Limitations and Requirements for Scheduled Conferencing, page 36 are complete.
- Review the best practice guidelines for Recommended Best Practices, page 18.

Process

Task 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 context-sensitive help or *Cisco TelePresence Management Suite Administrator Guide* at Cisco TelePresence Management Suite (TMS) Maintain and Operate Guides page.

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

Task 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 an IP zone for TelePresence Conductor.

Task 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.

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 (recommended).

Using dedicated bridges for scheduling

If you opt to use dedicated bridges for scheduled conferences, 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 instant/escalated conference.

Task 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.

Task 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*.

Task 6: Configure conference aliases in TelePresence Conductor

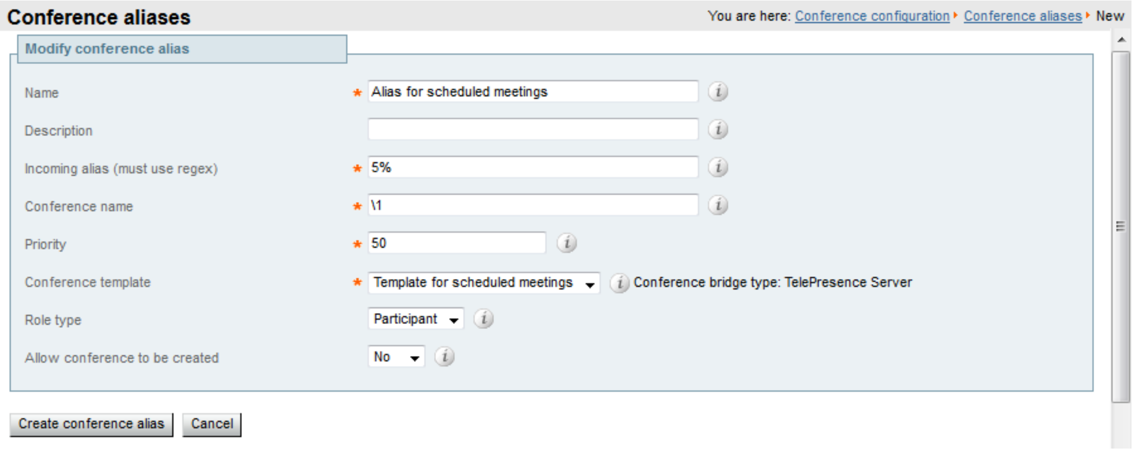
Define one or more TelePresence Conductor aliases to reflect your scheduled conferencing requirements.

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.

Figure 7 Example alias settings for Conductor



Conference aliases

You are here: Conference configuration ▸ Conference aliases ▸ New

Modify conference alias

Name	* Alias for scheduled meetings
Description	
Incoming alias (must use regex)	* 5%
Conference name	* \1
Priority	* 50
Conference template	* Template for scheduled meetings — Conference bridge type: TelePresence Server
Role type	Participant
Allow conference to be created	No

Task 7: Configure conference aliases in Cisco TMS

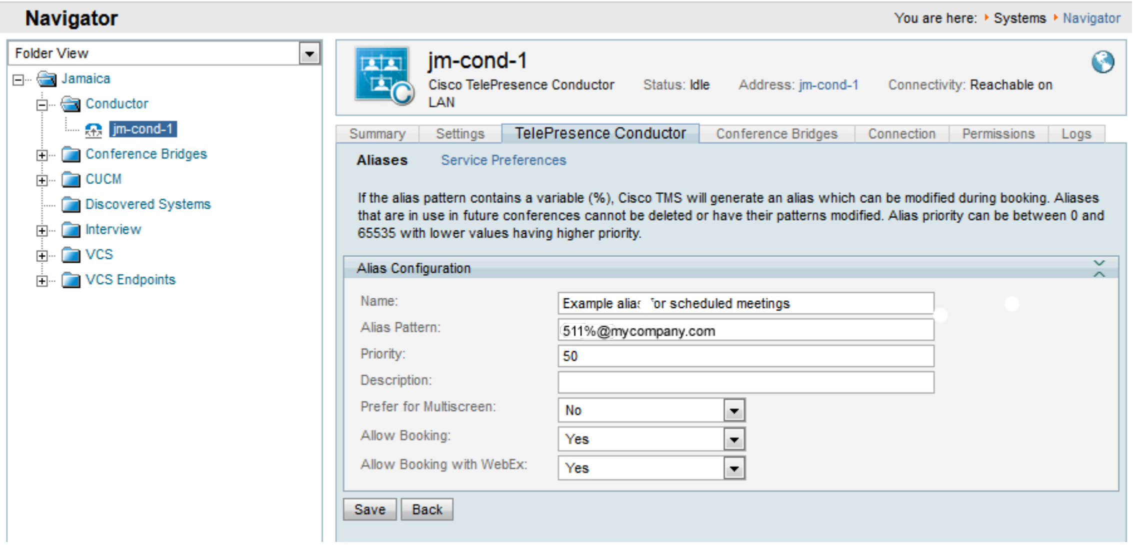
In Cisco TMS, go to **Systems > Navigator >** select the TelePresence Conductor **> Aliases** and select **New**.

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.

Figure 8 Example alias settings for Cisco TMS



jm-cond-1

Cisco TelePresence Conductor Status: Idle Address: jm-cond-1 Connectivity: Reachable on LAN

If the alias pattern contains a variable (%), Cisco TMS will generate an alias which can be modified during booking. Aliases that are in use in future conferences cannot be deleted or have their patterns modified. Alias priority can be between 0 and 65535 with lower values having higher priority.

Alias Configuration

Name: Example alias for scheduled meetings
Alias Pattern: 511%@mycompany.com
Priority: 50
Description:
Prefer for Multiscreen: No
Allow Booking: Yes
Allow Booking with WebEx: Yes

Task 8: Edit Service Preferences in Cisco TMS (optional)

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.

If you set a value over 100% then TMS allows conferences to be scheduled beyond the potential real-life capacity. If you set 120% for example, TMS adjusts its (logical) resources available for scheduling upwards by 20%. Over-allocating capacity (greater than 100%) might be a good idea if scheduling patterns and actual usage indicate significant idle resources, even when all resources are booked.

Examples

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. Over-allocating 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 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).

Task 9: Add conference bridges in Cisco TMS (optional)

If you want to do so, there are some advantages in optionally configuring TelePresence Conductor-managed conference bridges in Cisco TMS. See Conference Bridges in Cisco TMS, page 35

Task 10: Configure TelePresence Conductor settings in Cisco TMS

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

Task 11: Schedule the conferences

Note: This guide describes the Cisco TMS **Booking > New Conference** method to schedule conferences. Other methods available include Smart Scheduler through Cisco TMSPE, Microsoft Outlook through Cisco TMSXE, the Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA), and the Cisco TMS Booking API for customer groupware scheduling.

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.

More Information

- *Cisco TelePresence Management Suite Administrator Guide*
- *Cisco TelePresence Conductor Administrator Guide*
- *Cisco TelePresence Conductor API Guide*
- *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide*
- *Cisco TelePresence Conductor with Cisco TMS Deployment Guide*

Managing Personal CMR Conferencing

About 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.

Scheduling with Personal CMRs

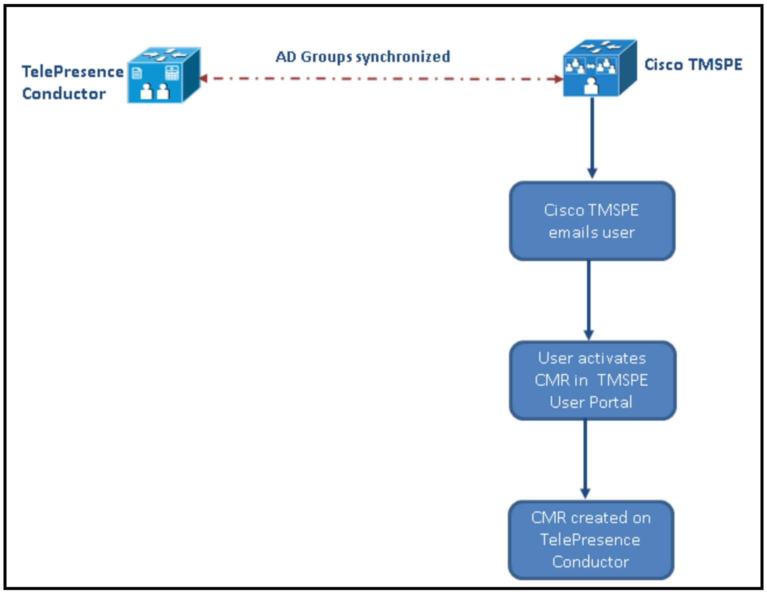
Users cannot schedule meetings to their Personal CMRs via the Cisco TMSPE user portal. However, when they schedule meetings through Microsoft Outlook they can include their Personal CMR for the meeting simply by adding the CMR alias to the “Location” field in the meeting invite.

Enabling Personal CMRs - Workflow Summary

To enable Personal CMRs, you define an API-enabled *User* on each TelePresence Conductor or cluster. Then in Cisco TMSPE you add the TelePresence Conductor *User*, create one or more CMR templates to specify the base dial plan for CMR URIs and numeric aliases, and apply the templates to Active Directory user groups. 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. The CMR is created on TelePresence Conductor when the user activates it. Detailed configuration steps are in the process below.

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.

Figure 9 Workflow for Personal CMRs



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.

Enabling Personal CMRs - Process

Task 1: Create a TelePresence Conductor User with API Access

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*

Task 2: Add the TelePresence Conductor API User to Cisco TMSPE

1. In Cisco TMS, go to **Systems > Provisioning > Users** (to access Cisco TMSPE).
2. Click **TelePresence Conductor Settings**.
3. Click **Add New**.
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.
5. Click **Save**.

Task 3: Enable WebEx for Personal CMRs (Optional)

If you have CMR Hybrid, you can optionally enable it in Personal CMRs to allow joint participation by Cisco WebEx and TelePresence users. You can do this as a separate task later, as described in Using CMR Hybrid with Personal CMRs, page 57, and regenerate the CMRs at that point. Or you can do it now, before you define the CMRs.

1. In Cisco TMS, go to **Administrative Tools > Configuration > Provisioning Extension Settings** (to access Cisco TMSPE).
2. Under **Collaboration Meeting Room**, set **Allow WebEx Connections** to *Yes*.
3. Click **Save**.

If you do it now, remember to check **Include WebEx** when you create the CMR templates in the next step.

Task 4: Create CMR Templates

1. In Cisco TMS, go to **Systems > Provisioning > Users** (to access Cisco TMSPE).
2. Under **Collaboration Meeting Room Templates**, create one or more templates as required.
   - 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.
   - You can also specify whether the CMR owner can distinguish between host and guest roles (see Using Host and Guest Roles in Personal CMRs, page 49).

Task 5: Apply the CMR Templates to Groups

In Cisco TMS, go to **Systems > Provisioning > Users** (to access Cisco TMSPE). Choose the relevant group, then select the button for the required template in the **Active** column.

Task 6: Enable Monitoring for Personal CMRs

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.

See the Cisco TMS context-sensitive help or *Cisco TelePresence Management Suite Administrator Guide* at Cisco TelePresence Management Suite (TMS) Maintain and Operate Guides page.

Task 7: Wait for Personal CMRs to Synchronize or Manually 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 straight away) you can manually synchronize the CMRs, as described here.

If you are upgrading an existing system and you want to manually synchronize, take care to do the synchronization at a time when it will have minimum impact on existing CMR users.

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

You have now completed all tasks to enable CMR conferencing. Assuming you have completed the relevant tasks in Connecting TelePresence Conductor, page 28, you can now use the following conference methods:

- Personal CMRs
- Multiway conferences
- Scheduled conferences

Task 8: Users Can Now Activate Their CMRs

This step does not involve the administrator. 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.

More Information

For guidance about subsequent administrator-level changes to Personal CMR configurations, see Managing Administration Changes to Personal CMRs, page 52.

For details about the TelePresence Conductor Provisioning API, see *Cisco TelePresence Conductor Product Programming Reference Guide* at Cisco TelePresence Conductor Programming Guides page.

For details about CMR configuration settings, see *Deploying Collaboration Meeting Rooms* at Cisco TelePresence Management Suite (TMS) Configuration Guides page.

Using Host and Guest Roles in Personal CMRs

When creating a template for Collaboration Meeting Rooms, the administrator can choose whether or not the CMR owner will be able to distinguish between host and guest participants.

Host Privileges

The participant or participants connecting to a CMR as a host can connect at any time regardless of whether there are other participants in the room.

A PIN may be required for them to join, depending on the configurations made by the administrator and the CMR owner.

Depending on the bridge used, participants connecting as guests may be required to wait until a host joins the meeting before they will be allowed into the CMR.

- Cisco TelePresence MCU Series: guests must always wait for a host to join.
- TelePresence Server: the policy is determined by the **Guest Lobby** setting of the CMR.

Process for Enabling the Guest Role in a CMR

On the template of the CMR:

- Check **Allow Guest Role**.
  To make the guest role optional to CMR owners, you must leave the host PIN requirement as `0` (optional).
- Select whether to enable **Guest Lobby**, which means guests must wait in the lobby unless at least one host is present in the CMR. When a conference is initiated, automatic dial out is initiated for all the favorite endpoints that are part of the conference. In this case, the favorite participant will join the conference first and then subsequently all the remaining participants in the lobby will join the conference.
  This setting will apply to all rooms based on the template and is not configurable for the CMR owner.

When the guest role is allowed:

- The guest role will only be used if the administrator or CMR owner set a PIN requirement for the host.
  If no PIN is set for the host, everyone is allowed into the CMR automatically with host permissions.
- If a PIN is set for the host, but not for the guests, guests will be asked to press `#` to connect to the CMR.
- You can only have a PIN requirement for the guest if there is also a PIN requirement for the host.

Process for Disabling the Guest Role in a CMR

To make all participants have the same PIN requirements and the same privileges, uncheck **Allow Guest Role** on the CMR template.

When the guest role is not allowed, all participants are treated as hosts and can connect at any time regardless of whether there are other participants in the room.

Configuring Conference Services

Managing Multiparty Licensing

This section applies 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.

Requirements for Multiparty Licensing

- Cisco TelePresence Server conference bridges, with software version 4.2 or later and running in remotely managed mode.
- TelePresence Conductor, with software version XC4.0 or later.
- All connections between TelePresence Conductor and the TelePresence Servers must use HTTPS.
- Cisco TMSPE, with software version 1.5 or later. Cisco TMSPE is not required, although we recommend it to allow users to have a vanity URI/number.

Licenses on Clustered Conductors

The licenses (option keys) can be installed on any node in a clustered Conductor configuration. If the node fails, the option keys remain valid for 30 days.

Installing the Licenses and Enabling Multiparty Licensing

You enable Multiparty Licensing through TelePresence Conductor, by applying the purchased licenses to Conductor and switching on the Multiparty Licensing option:

1. Have the option key codes for the purchased licenses available. (Option keys are obtained by registering the Product Authorization Key (PAK) from the sales order, at http://www.cisco.com/go/license)
2. In TelePresence Conductor, go to **Maintenance > Options**.
3. Paste the first option key code into the **Add option key** field.
4. Click **Add option**.
5. Repeat if you have further licenses and option key codes.
6. Set **Multiparty Licensing for TelePresence Servers** to *Enabled*.

Applying Licenses to Users

You apply Multiparty Licenses to users through the template assigned to their associated user group in Cisco TMS:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. Under **Collaboration Meeting Room Templates**, select the template concerned.
3. Set the **Multiparty License Mode** drop-down to *Shared Multiparty*. Ignore the *Personal Multiparty* option, which does not apply in Cisco VCS-based deployments.

Users will now consume a Shared Multiparty (SMP) license for their active conferences.

Monitoring License Use

To view how many SMP licenses are installed and their peak usage in the last 60 days:

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

Managing Administration Changes to Personal CMRs

This section explains how to make administrator-level changes to the Personal CMR configuration in your deployment.

Before You Start

Caution: Some changes will impact CMRs and may cause disruption to users.

We strongly recommend that administrators fine-tune templates as much as possible before applying them to groups and allowing users to create their own CMRs.

If you need to make changes to templates after making CMRs available to users, we recommend using maintenance windows or advising users in advance when they should avoid creating or changing CMRs. Where appropriate notify users about the likely impact of the changes.

Process

Task	Instructions
Modifying template settings	You can change the settings for a template that has already been assigned to a group. The changes will impact the available CMR settings in the affected group(s). 1. In Cisco TMS, go to **Systems > Provisioning > Users > Collaboration Meeting Room Templates**. 2. In the template list, click the pencil icon next to the required template, make the changes and click **Save**. Repeat as necessary for any other templates that need modifying. 3. The counter next to **Check sync status** indicates how many CMRs are out of sync with the modified templates. Click **Regenerate CMRs** to synchronize the change on TelePresence Conductor. The **SIP Alias Pattern** will always regenerate. The **Numeric Alias Pattern** never regenerates once it is set on a CMR. If the template changes make the PIN policy stricter, Cisco TMSPE generates a new PIN for any non-compliant CMRs when the changes are synchronized (PINs are generated for all CMRs that do not meet the new criteria).
Removing CMR entitlement	Set the CMR template for the group to *None*. This removes CMR capabilities from the users in that group. **Note:** To set sub-groups to *None*, the parent root group must be set to *None*. 1. In Cisco TMS, go to **Systems > Provisioning > Users** 2. Select the relevant group. 3. Under **Collaboration Meeting Room Templates**, click *None* in the Active column. 4. In the **Change Template for Group** popup, click **Yes**.
Selecting a different template for a group	1. In Cisco TMS, go to **Systems > Provisioning > Users** 2. For the relevant group, select the button for the required template in the **Active** column.

Deleting templates	1. In Cisco TMS, go to **Systems > Provisioning > Users > Collaboration Meeting Room Templates** 2. Click the red deletion icon next to the template name in the list. You cannot delete a template that is associated with an existing CMR.
Deleting users	If you delete a user from the user base, the user's CMR is automatically deleted.
Moving users between groups	If a user's group changes in the user base (normally due to changes in Active Directory) their assigned CMR template will also change if the new group has a different template. Cisco TMSPE will register the change during the next health check. Or you can run a health check manually from the **Provisioning Extension Diagnostics** page (**Run Health Check**). The user's CMR will be displayed as out of sync. To synchronize, click **Regenerate CMRs** to have the change reflected on TelePresence Conductor.
Manually synchronizing all Personal CMRs	If you make changes to Personal CMRs and you want to use the Personal CMRs straight away, you can synchronize them manually. To do this: 1. In Cisco TMS, go to **Systems > Provisioning > Users**. 2. Under **Collaboration Meeting Room Templates**, click **TelePresence Conductor Settings**. 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'). 4. In the dialog window that opens, click **Synchronize Now**.

More Information

For details about the TelePresence Conductor Provisioning API, see *Cisco TelePresence Conductor Product Programming Reference Guide* at Cisco TelePresence Conductor Programming Guides page.

For details about CMR configuration settings, see *Deploying Collaboration Meeting Rooms* at Cisco TelePresence Management Suite (TMS) Configuration Guides page.

Configuring TMS Support for Two-Node Conductor Clusters

This feature applies if you use two-node clustered TelePresence Conductors (three nodes are not supported). You can configure Cisco TMS to automatically switch over to the subordinate Conductor if the primary Conductor node fails. TMS monitors the status of the primary node through a mix of polling and feedback requests. Failover happens only while the primary node is down, and TMS reroutes to the primary Conductor when it's available again.

While the primary node is down you can continue to schedule meetings as normal, without any manual intervention on the TMS. Some Conference Control Center functions are also available. If the primary node is still down at the scheduled start time, TMS switches the meeting to the subordinate node. Note that TMS does **not** display the subordinate node as an available bridge for booking. Conductor cluster behavior remains unchanged - calls may drop and have to dial back into their meetings, and some services may be temporarily unavailable during the cluster's recovery from a node failure.

Cisco TMSPE and its associated functions do not failover.

All failover operations are logged (see TMS Logging for Conductor Failover, page 76).

The " primary Conductor" is mainly a concept in TMS rather than Conductor. TMS designates a specific Conductor node in any cluster as the primary Conductor. TMS will always use this node (or revert to it after a node failure) in preference to the subordinate node in the cluster.

Subject to proper configuration of the cluster in TelePresence Conductor, TMS automatically knows which Conductors are present in a cluster. However, you do need to manually add each Conductor in the cluster as a system in TMS.

Before You Start

The cluster must already be configured in TelePresence Conductor.

Please review the *Release Notes* on the CMR Premises solution documentation listing page before you use this feature.

We recommend using the same Conductor for Cisco TMSPE, and as the primary Conductor in Cisco TMS.

TMS automatically designates the primary node, as the Conductor with at least one conference bridge and an alias defined. (TMS only ever adds bridges to one Conductor in the cluster.)

The TMS **Systems > Navigator** page for Conductor systems displays the **TelePresence Conductor** and **Conference Bridges** tabs only for the primary node, not for the subordinate node.

The **Clustering** tab on the **Systems > Navigator** page lists the peers in a cluster, and their status. If the nodes are reachable and TMS can communicate with them normally, the status is *OK*. Otherwise the status is *Inaccessible*.

Process to Configure TMS

This is a summary of the steps in TMS. Detailed instructions are available in the *Cisco TelePresence Management Suite Administrator Guide* on the TMS Maintain and Operate Guides page.

1. Add the primary TelePresence Conductor as a system in TMS.
2. Configure an alias for the primary Conductor.
3. Add the conference bridges for the primary Conductor.
4. Add the subordinate Conductor as a system in TMS.

Using CMR Hybrid in Scheduled Conferences

This section describes how to enable CMR Hybrid for scheduled conferences in a CMR Premises deployment, for participation by Cisco WebEx and TelePresence users.

Before You Start

- The standard requirements for enabling scheduled conferences apply.
- SIP Early Offer messaging is the default. However, if you have a Unified CM in the network and it is required to support WebEx, you must ensure that Early Offer messaging is configured on the SIP trunks between the following elements:
  - Bridges used for calls between Early Offer-based services and the Cisco Expressway.
  - Any third-party call controller and the Cisco VCS Control.
  - Any Unified CM-managed endpoints and the Cisco Expressway. The entire path from the calling device to the service must be configured to support Early Offer.

    If you do not need external Early Offer-based services, then any Unified CMs may be configured for either Delayed Offer or Early Offer.

Process

Task 1: Configure TelePresence Applications for Cisco WebEx Support

If not already done, complete the first-time configuration steps in *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* on the Cisco TelePresence Management Suite (TMS) Configuration Guides listing page so that your Cisco TelePresence applications are enabled for Cisco WebEx-to-Cisco TelePresence interoperability. Detailed instructions and a first-time configuration checklist are provided in that guide.

Task 2: Configure Cisco WebEx Site Administration

If not already done, after the first-time configuration steps in Task 1 are complete you need to set up Cisco WebEx site administration, as described in *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* on the Cisco TelePresence Management Suite (TMS) Configuration Guides listing page.

Task 3: Book the Conferences (Users)

Now users can book conferences.

In Cisco TMS, go to **Booking > New Conference** and complete the relevant fields on the **Basic Settings** tab. Make sure **Include WebEx Conference** is checked and optionally create a **WebEx Meeting Password**.

When you save a conference, Cisco TMS emails you the meeting details with WebEx and TelePresence dial-in information. Depending on your site configuration you may also get emails from WebEx.

For details, see the chapter about scheduling CMR Hybrid meetings in Cisco TMS in *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* on the Cisco TelePresence Management Suite (TMS) Configuration Guides listing page.

Task 4: Forward the Meeting Details (Users)

Forward the meeting email issued in the previous step to the conference participants.

More Information

- For detailed information about Cisco TMS settings, see the context-sensitive help for Cisco TMS or *Cisco TelePresence Management Suite Administrator Guide*on the Cisco TelePresence Management Suite (TMS) Maintain and Operate Guides listing page.
- For detailed configuration steps to enable this feature, see *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide* on the Cisco TelePresence Management Suite (TMS) Configuration Guides listing page.

Using CMR Hybrid with Personal CMRs

If you have deployed CMR Hybrid, you can include WebEx in CMRs so that users may connect using either TelePresence or WebEx.

When enabled through the Collaboration Meeting Room template, a **Create WebEx Connection** button will appear on each user's CMR page on the TelePresence User Portal. The button allows the user to create a temporary WebEx connection for their CMR.

As the connection is temporary and will eventually time out, the portal page advises users to create the connection and distribute the WebEx details shortly before the meeting starts.

Before You Start

Before you can enable WebEx in CMRs:

- CMR Hybrid must be deployed. See *Cisco Collaboration Meeting Rooms Hybrid Configuration Guide* for details and instructions.
- The owner of each CMR must be a registered WebEx user associated with a current WebEx site with their own username and password. Otherwise, the **Create WebEx Connection** button will not appear for the user.
- If planning to change an existing template, read Managing Administration Changes to Personal CMRs, page 52.
- To prevent potential toll fraud issues, we recommend disabling **Call-back teleconferencing** on the WebEx site that is used for CMRs.

Process

You must enable WebEx for CMR before you can include the feature in one or more templates:

1. In Cisco TMS, go to **Administrative Tools > Configuration > Provisioning Extension Settings**.
2. Under **Collaboration Meeting Room**, set **Allow WebEx Connections** to *Yes*.
3. Go to **Systems > Provisioning > Users**.
4. Select an existing template for editing or create a new template.
5. Check **Include WebEx**.
6. Click **Save**.
7. Click **Regenerate CMRs**.

Setting Up Cascading for Large-Scale or Critical Meetings

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 TelePresence Conductor.

Before You Start

In the case of cascading for scheduled conferences, the standard requirements for enabling scheduled conferences apply (see How to Enable Scheduled Conferencing, page 40).

- Cascading is not supported from one conference bridge to another bridge that is outside the boundaries of the local enterprise network.
- Multistream video is not available over cascade links.
- 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 based on the configured maximum number of cascades. The resources are reserved whether or not they are actually used.

  For this reason, we recommend using the cascade option sparingly. Typically for large-scale meetings or for Personal CMR / rendezvous conferences used by VIP personnel.
- You should not enable cascading if it is critical to have certainty about resource availability. Such as a conference bridge that is reserved for scheduled conferences only.
- Cascade links share only a single screen of video between TelePresence Servers.

Process for CMR Conferences

Note: This process uses the Cisco TMSPE provisioning extension of Cisco TMS. If your deployment does not use Cisco TMSPE, you can instead use the TelePresence Conductor to configure cascading, as described in Task 2: Enable Cascading in TelePresence Conductor, page 59.

Task 1: Create a Cascade-Enabled CMR Template

1. In Cisco TMS, go to **Systems > Provisioning > Users** to access Cisco TMSPE.
2. Under **Collaboration Meeting Room Templates** create one or more templates as required.
3. Check the **Allow Cascading** check box.
4. Specify the maximum number of cascades allowed for a conference.

   If the maximum number of cascades is set to 2, up to 3 bridges can be used for the conference.

   A small number of cascades may result in insufficient resources, if the number of participants is large and the bridges have filled up.

   A large number of cascades will result in resources being used up for the cascade links and will reduce the user experience for participants on the cascade bridges.

Task 2: Apply the CMR Template to a Group

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. Under **Users and Groups**, choose the relevant group.
3. Under **Collaboration Meeting Room Templates**, select the radio button for the required template in the **Active** column.

Process for Scheduled Conferences

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.

Task 1: Book the Scheduled Conference as Normal in Cisco TMS

Add the TelePresence Conductor to the conference (unless it is defined as the default MCU).

Task 2: Enable Cascading in TelePresence Conductor

1. In TelePresence Conductor, go to **Conference configuration > Conference templates**.
2. Select an existing conference template or click **New**.
3. Set an appropriate value for **Maximum number of cascades**.

   A value of 0 disables cascading.

   If the maximum number of cascades is set to 2, up to 3 bridges can be used for the conference.

   A small number of cascades may result in insufficient resources, if the number of participants is large and the bridges have filled up.

   A large number of cascades will result in resources being used up for the cascade links and will reduce the user experience for participants on the cascade bridges.

Localizing and Customizing the Solution

For TelePresence Server-hosted conferences, the supplied conference prompts (voice and text) are available in various languages in addition to the default English (U.S.). The TelePresence Conductor interface lets you select a language for the prompts from the **Conference configuration > Global settings**. These take effect at the Conductor level for all bridges managed by that Conductor.

You can optionally create and use your own customized conference prompts. These override the corresponding settings in Conductor, and take effect at the conference template level. They are managed through the conference bridge API.

You may want to use your own prompts if:

- You need a language that we don't supply.
- You want to change the language per conference template rather than per TelePresence Conductor.

The supplied languages include:

- Chinese (Simplified)
- Chinese (Traditional)
- French (France)
- French (Canada)
- Italian
- Korean
- Polish
- Portuguese (Brazil)
- Turkish

The *TelePresence Conductor Administrator Guide* has more information about the Cisco-supplied prompts, with a full list of the available languages.

Using Your Own Prompts

Prompts are customized using TelePresence Server API parameters. You apply the API parameters through Conductor, using JSON commands in the **Advanced Parameters** for the relevant conference templates.

For voice prompts, the audio files must be hosted on an external HTTP/HTTPS server. You specify the URL of the relevant audio file for a voice prompt, in the JSON command.

An example of how to use JSON to define custom parameters for the TelePresence Server is provided in the *TelePresence Conductor Administrator Guide*.

The following prompts are customizable:

Table 8 TelePresence Server Voice and Text Prompts

Voice		Text		
JSON Name	Message	JSON Name	Message	Comment
customPINEntryAudio	Please enter the security PIN followed by #.	customPINEntryMessage	Please enter the security PIN followed by #.	Used if PIN for all is required.

Table 8 TelePresence Server Voice and Text Prompts (continued)

Voice		Text		
JSON Name	Message	JSON Name	Message	Comment
customOptionalPINEntryAudio	Please enter the security PIN followed by #, *[one second pause*] or press # to continue.	customOptionalPINEntryMessage	Please enter the security PIN followed by # or press # to continue.	Used if no pin for guests is required.
customPINIncorrectAudio	You have not entered the PIN correctly, please try again.	customPINIncorrectMessage	You have not entered the PIN correctly, please try again.	
customPINFailedExitAudio	You have not entered the PIN correctly. This call will be disconnected.	customPINEntryFailedMessage	You have not entered the PIN correctly. This call will be disconnected.	
welcomeScreenAudio	Welcome to the conference. *[one second pause]*	welcomeScreenMessage	Welcome to the conference.	Text is only displayed if the conference does not have a name.
customOnlyParticipantAudio	*[one second pause]* You are the only call in this conference.	customVideoOnlyParticipantMessage	You are the only call in this conference.	This prompt plays one second of silence before any speech is heard. This will be fixed in a future release. Bug ID: CSCuz05735
customWaitingForChairAudio	Please wait until the host joins.	customWaitingForChairMessage	Please wait until the host joins.	

Table 8 TelePresence Server Voice and Text Prompts (continued)

Voice		Text		
JSON Name	Message	JSON Name	Message	Comment
NA	NA	customConferenceEndingMessage	The scheduled meeting ends in 1 minute.	
customConferenceEndedExitAudio	The conference has ended. Thank you for joining.	customConferenceEndedExitMessage	The conference has ended. Thank you for joining.	'Thank you for joining.' will be moved to the **customDisconnectPlatitudeMessage** in a future release. Bug ID: CSCuz05731
customParticipantDisconnectedExitAudio	This call has been disconnected. Thank you for joining.	customParticipantDisconnectedExitMessage	This call has been disconnected. Thank you for joining.	'Thank you for joining.' will be moved to the **customDisconnectPlatitudeMessage** in a future release. Bug ID: CSCuz05731
NA	NA	customMutedCanUnmuteMessage	Your audio has been muted. Press *6 to unmute.	
NA	NA	customMutedCannotUnmuteMessage	Your audio has been muted.	
NA	NA	customDisconnectPlatitudeMessage		'Thank you for joining.' will be moved to this message in a future release. Bug ID: CSCuz05731
NA	NA	customConferenceAutoDisconnectExitMessage	[empty]	Blank by default

Recommendation

Before changing any conference prompts settings, make sure there are no conferences running on the Conductor.

More Information

- For more information about the Cisco-supplied languages, see the *TelePresence Conductor Administrator Guide* on the TelePresence Conductor Maintain and Operate Guides listing page.

- For information about the API commands to customize voice or text prompts, see the *TelePresence Server API Reference Guide* on the TelePresence Server Programming Guides listing page.
- For information about recording voice prompts, see the article on the TelePresence Server Maintain and Operate TechNotes listing page.

Configuring Conference Features

This section assumes that basic configuration for the CMR Premises solution is complete. Typically you will already have done some of the tasks in this section as part of the initial implementation.

The tasks are grouped here for administrator convenience, from the view of enabling individual solution features rather than the overall solution as a whole.

Changing the Conference Placement Method

This section describes how to optionally specify the method that Conductor uses to select bridges for conferences:

- `Favor Scheduled`: selects the bridge with the fewest conferences currently in progress (better for conferences that start at the same time). This is the default setting.
- `Favor CMRs`: selects the bridge with the most spare capacity (better for conferences with staggered start times).

`Favor Scheduled` treats all bridges equally so that the smaller bridges in the pool get the same number of conferences as the bigger bridges. A disadvantage to this approach is that meetings on the smaller bridge have a greater risk of failing to accommodate additional participants.

Example 1: Two bridges - each with 10 ports. Bridge A has a 4-port conference started in the previous hour (leaving 6 available ports). Three new calls come in to three new conferences, none of which reserves additional resources. They are all placed on Bridge B (consuming 3 ports). Five minutes later, each of those conferences tries to grow to 4 ports (requiring a total 12 ports) and each runs out of room. If one conference had been placed on Bridge A, they all would have fit.

In this first example, if `Favor Scheduled` were selected, the bridge with the fewest conferences currently running would be selected. The first new conference would be placed on Bridge B, and one of the remaining new conferences would be placed on Bridge A and the other on Bridge B, so that all conferences would fit.

Example 2: Same two bridges as Example 1. Bridge A has an 8-port conference (leaving 2 available ports). The three new conferences only grow to 3 ports. Like Example 1, the first is placed on Bridge B and one of the remaining two is placed on Bridge B and the other on Bridge A. However, in this case, the one placed on Bridge A doesn’t fit.

In this second example, if `Favor CMRs` were selected, all conferences would fit if each conference grew to its full size before the next conference was placed.

To change the conference placement method

1. In Conductor, go to **Conference configuration** > **Global settings**.
2. Select the required conference placement setting.

Changing the Switching Mode on the TelePresence Server

The TelePresence Server supports two different switching modes for displaying speakers from telepresence rooms:

- Segment-switched (default)
- Room-switched

This section describes how to optionally change the TelePresence Server mode.

Note: Conference participants with Cisco TelePresence IX5000, TX Series, or Cisco CTS endpoints can manually choose between segment-switched or room-switched mode.

Changing the Mode on Cisco TMS-Managed Conferences (Administrator)

To change the mode for Personal CMR conferences (which are managed through Cisco TMS):

1. In Cisco TMS go to **Systems > Provisioning > Users**.
2. Under **Collaboration Meeting Room Templates** click the edit button for the appropriate CMR template.
3. Check **Advanced Parameters**.
4. Type the following JSON command into the **Advanced Parameters** field:

   `“callAttributes: {“displayLayoutSwitchingMode”: <******>}”` where `<******>` should be specified as `switchingRoomSwitched` or `switchingSegmentSwitched`

Changing the Mode on the TelePresence Conductor (Administrator)

For rendezvous conferences (which are managed with TelePresence Conductor) the **Segment switching** field in the conference template determines the switching mode. To change the mode:

1. In TelePresence Conductor go to **Conference configuration > Conference templates**.
2. Click the appropriate conference template.
3. Change the **Segment switching** setting as appropriate. *Yes* for segment switching or *No* for room switching.

Changing the Mode on Endpoints (User)

Conference participants with Cisco CTS or TX Series endpoints can manually choose between segment-switched or room-switched mode during a conference.

Managing IX Protocol Settings

The iX protocol is required for these solution features:

- ActiveControl
- Multistreaming (for enhanced layouts)

This table describes the default iX settings in the solution, and where the settings can be configured for each affected component.

Table 9 iX configuration settings

Component	IX setting...
CE-based endpoints	Default is Auto. ActiveControl is enabled if the call control system to which the endpoint is registered supports the iX protocol and disabled otherwise. No action needed unless you have changed the default.
TC-based endpoints	Default is Auto. ActiveControl is enabled if the call control system to which the endpoint is registered supports the iX protocol and disabled otherwise. No action needed unless you have changed the default.
TelePresence Server	Enabled by default. No action needed unless you have changed the default.
TelePresence Conductor	Enabled by default. No action needed unless you have changed the default. You can verify the current Conductor setting as follows: 1. Go to the **Advanced parameters** for the template applied to the TelePresence Servers. 2. The **Enable iX protocol** field should be set to *True*.
Cisco TMSPE (for Personal CMRs)	Enabled by default for Personal CMRs. No action needed unless you have changed the default. You can verify the current Conductor setting as follows: 1. In Cisco TMS, go to **Systems > Provisioning > Users** and select the relevant CMR template. 2. On the **Edit CMR Template** page, check the check box for **Custom Parameters**. 3. In the **Advanced parameters** field, enter `{"callAttributes": {"iXEnabled": true}}` and click **Save**.
Cisco VCS (per neighbor zone)	To disable iX pass-through for a neighbor zone that does not support iX, configure each zone with a custom zone profile as follows: 1. Select the zone (**Configuration > Zones > Zones**). 2. In **Advanced parameters**, for **Zone profile**, choose *Custom* if it is not already selected. The zone profile advanced configuration options display. 3. From the **SIP UDP/IX filter mode** drop-down list, choose `On` and click **Save**.

Examples of iX Call Handling Behavior

Table 10 Call handling summary for calls that contain an iX header

Scenario	Outcome
Unified CM 8.x or earlier	Calls fail
Unified CM 9.x earlier than 9.1(2)	Calls handled normally but no ActiveControl
Unified CM 9.1(2)	Calls handled normally plus ActiveControl
Endpoint - if no support for iX and no SDP implementation	Endpoint may reboot or calls may fail

Using ActiveControl

ActiveControl allows participants in a video conference to view and change some aspects of the conference directly from the Touch controller on their endpoints. Users can see a list of participants and other conference information, and on certain models they can also change the local layout display and disconnect other participants.

Limitations and Requirements

- You need to configure the Cisco Expressway / Cisco VCS to disable iX pass-through for any neighbor zone that does not support the iX protocol (that is, connects to an external network or connects internally to a Unified CM running 8.x or earlier). For configuration details, see Managing IX Protocol Settings, page 67.
- Endpoints need Touch controllers, and software version TC7.1.3 or later or CE 8.0 or later. ActiveControl is not supported on other endpoints.
- If an ActiveControl-enabled call traverses a Unified CM trunk with a Unified CM version lower than 9.1(2), the call may fail. ActiveControl should not be enabled on older Unified CM trunks (Unified CM 8.x or earlier).
- The ActiveControl feature on the TelePresence Server supports up to 500 participants.
- ActiveControl/iX protocol traffic is not encrypted.
- ActiveControl is a SIP only feature. H.323 interworking is not supported.

Caution: Care is needed with connections to external networks which may not support the iX protocol (including systems running Unified CM 8.x or earlier). To avoid unpredictable results and call failures in the event of mismatched iX capabilities, you should disable the iX protocol for all such outward connections. See Limiting ActiveControl in External Connections, page 70 for instructions.

Limiting ActiveControl in External Connections

The iX protocol is advertised as an application line in the SIP Session Description Protocol (SDP). Extensions to the SIP SDP are not fully supported in some older systems, which has implications for CMR Premises networks that connect to external networks or to older Unified CMs (Unified CM 8.x or earlier). No issues occur with iX in Unified CM 9.1(2) or later, or with iX in Cisco VCS systems. However, if you are enabling ActiveControl in CMR Premises networks which interface to older Unified CMs (8.x and earlier) or to third-party networks (business-to-business), you must follow the instructions in this section carefully to isolate the iX protocol traffic from systems that do not support it. Failure to do so may lead to unpredictable consequences, including call failures.

In situations where the far end network is not known or is known to have devices that do not support iX, it may be safest to disable iX on connections leaving the known environment, as follows:

Deployments which connect to external networks or connect internally to older Unified CM versions.

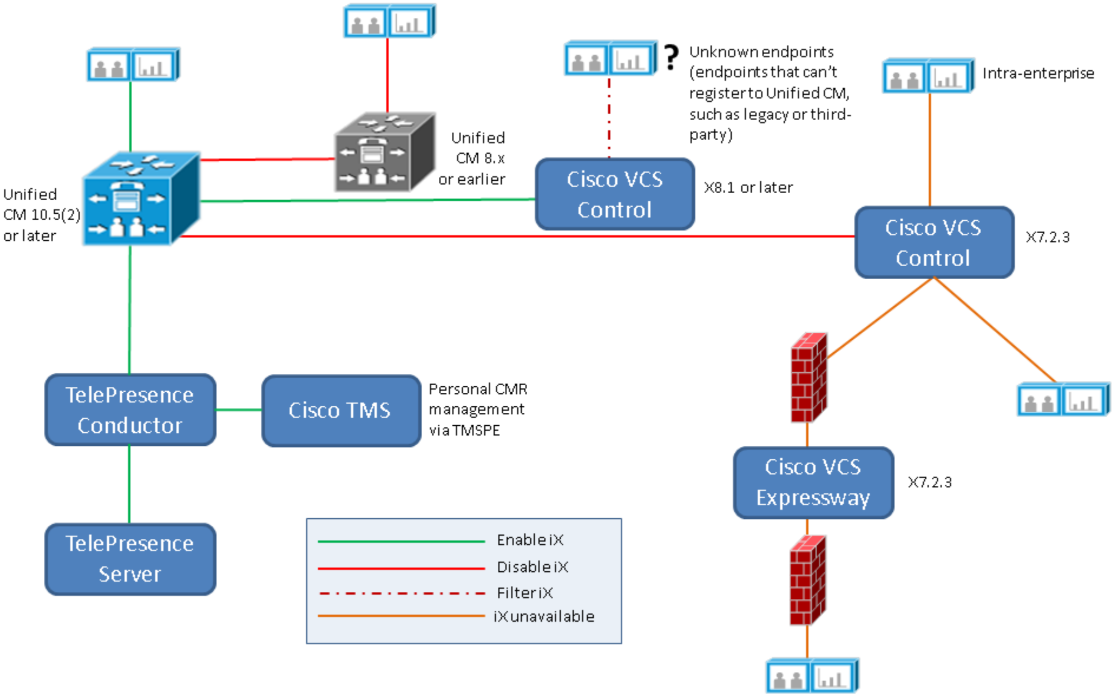
- Starting in Cisco VCS X8.1, you can turn on a zone filter to disable iX for INVITE requests sent to external networks or older Unified CM systems. (By default, the filter is off.)
- With version X7.2.3, we recommend that you leave iX disabled throughout the CMR Premises network. (In some situations it is possible to enable iX in X7.2.3 with workarounds, but this should only be done with guidance from Cisco Technical Support.)

Table 11 Summary of iX configuration requirements in the CMR Premises network

Network connection from...	Network connections to...	Can you enable iX (ActiveControl)?
Unified CM 10.5(2)	Unified CM 9.x or later	Can be enabled on this trunk. May require disabling on trunks from this second Unified CM.
	Unified CM 8.x or earlier	Disable on this trunk from the first Unified CM.
	Third-party networks	Disable on this trunk from the Unified CM.
	Cisco VCS versions prior to X8.1	Disable on this trunk from the Unified CM if this route is used for trunks to third-party networks or to Unified CM 8.x or earlier systems. Can be enabled if only Unified CM 9.x or Cisco VCS systems can be reached via this trunk.
	Cisco VCS X8.1 and later	Can be enabled on this trunk if you turn on the iX filter in Cisco VCS to neighbor zones connected to the third-party networks or Unified CM 8.x or earlier systems.
Cisco VCS X8.1.1 or later	Unified CM 9.x or later / Cisco VCS systems only	Yes. Enable as you wish.
	Any other devices, including Unified CM 8.x or earlier	Turn on the iX filter on the neighbor zones between the Cisco VCS and these devices to remove the iX protocol line. (Filters were introduced in Cisco VCS X8.1.)
Cisco VCS X7.2.3	Unified CM 9.x or later / Cisco VCS systems only	Yes. Enable as you wish.
	Any other devices, including Unified CM 8.x or earlier	No. Disable throughout the network (default).

Illustrations of iX configuration settings

Figure 10 Where to enable/disable iX in outward connections from Unified CM-managed systems



Note: This illustration does not show any business-to-business scenarios. The elements shown are all sited within the local enterprise.

Figure 11 Example iX configuration in a Unified CM Session Management Edition deployment

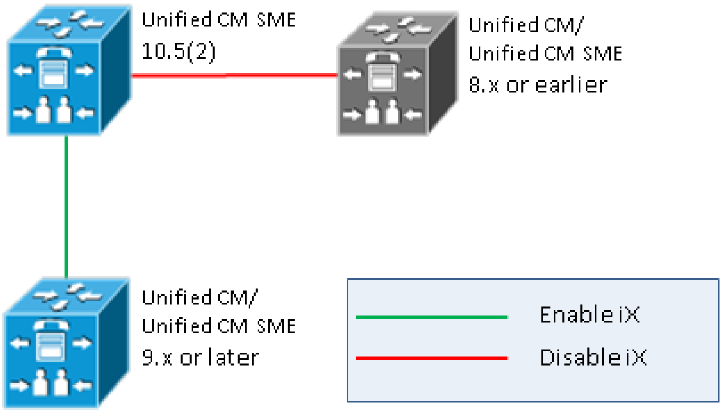
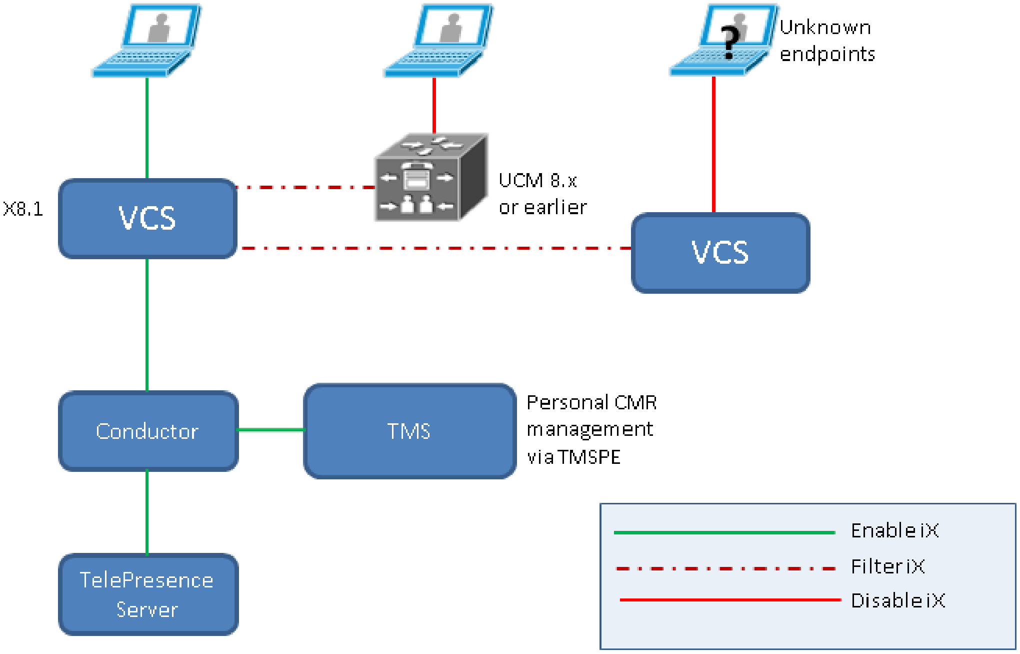


Figure 12 Where to filter iX in outward connections from Cisco VCS-managed systems (Cisco VCS X8.1 and later)



Managing Multistream Video (Supports Enhanced Layouts)

Multistreaming is enabled by default in most solution products, but some configuration is required as described here.

Requirements

- Multistream-capable endpoints running software version CE8.0 or later (Cisco TelePresence MX200 G2, MX300 G2, MX700, MX800, SX20, SX80). *Multistreaming is off by default in the endpoints.*
- Cisco TelePresence Server on Virtual Machine, Cisco Multiparty Media 310/320, or Media 820 running TelePresence Server 4.2 software or later.
- The iX protocol is required for this feature to work to endpoints. iX is on by default in all relevant components (see Managing IX Protocol Settings, page 67).
- You need to configure the Cisco Expressway / Cisco VCS to disable iX pass-through for any neighbor zone that does not support the iX protocol (that is, connects to an external network or connects internally to a Unified CM running 8.x or earlier). For configuration details, see Managing IX Protocol Settings, page 67.
- Do not disable the iX protocol in any conference templates in Conductor or in any CMR templates in Cisco TMSPE.

Limitations

Some restrictions currently apply to enhanced layouts. See the *Limitations* section of the *CMR Premises Release Notes* on the CMR Premises solution documentation web page.

Enabling Multistreaming

Task 1: Endpoints

Configure the endpoints to support multistreaming. Go to **System Configuration > Conference** and set **Multistream Mode** to *Auto*.

Task 2: TelePresence Server

The TelePresence Server supports multistreaming by default and you do not need to configure it.

Disabling Multistreaming

You can optionally switch off multistreaming. Either for individual endpoints (assuming you have previously configured them for multistreaming), or in the Conductor conference templates or the CMR templates in Cisco TMSPE. You can also disable multistreaming at neighbor zone level, by switching off the iX protocol for a specific neighbor zone in VCS. However, this is not recommended as it *also has the effect of disabling ActiveControl*. In which case non-multistream endpoints cannot support ActiveControl for participant lists and conference control.

To disable multistreaming for individual endpoints:

On the endpoint, go to **System Configuration > Conference** and set **Multistream Mode** to *Off*.

To disable multistreaming in Conductor templates:

1. In Conductor, go to **Conference configuration > Conference templates** and select the first conference template.
2. In the **Advanced parameters** section, click **Edit**. The **Advanced Template Parameters** page opens.
3. In the **Custom parameters** field, type the following JSON command:

   ```
   {“callAttributes":{“multistreamMode":"multistreamOff"}}
   ```

4. Select the check box next to the **Custom parameters** field.
5. Repeat for other templates as required.

To disable multistreaming in CMR templates:

1. In Cisco TMS, go to **Systems > Provisioning > Users** (to access TMSPE).
2. In the Collaboration Meeting Room Templates section, select the first template and click the Edit icon.
3. Select the check box next to the **Advanced Parameters** field.
4. In the **Advanced Parameters** field, type the following JSON command:

```
{"callAttributes":{"multistreamMode":"multistreamOff"}}
```

5. Click **Save**.
6. Repeat for other templates as required.

Troubleshooting

If multistream video does not work, try these steps:

Element	Check that ...
Endpoints	**Conference > Multistream Mode** and **Conference > ActiveControl Mode** settings are enabled (set to *Auto*). iX protocol is enabled in the SIP profiles for the endpoints.
Unified CM	iX protocol is enabled on the relevant trunks.
TelePresence Conductor templates	iX protocol is enabled in the Advanced template parameter page.
Cisco TMSPE Personal CMR templates	iX protocol is enabled in the Advanced parameters field. Enter `{"callAttributes": {"iXEnabled": true}}`.
Various	Bandwidth values for the relevant links, endpoints and templates are valid. Multistream is disabled if the call rate drops below 512k.

Active Meeting Manager (Preview Feature)

The Active Meeting Manager (AMM) preview feature will be removed from the solution in an upcoming release. Customers are therefore advised not to deploy this feature.

You can optionally disable AMM in Cisco TMSPE so that users don't see it in their CMR portal pages. You may want to do this an interim measure until we remove the feature. To disable AMM:

1. In Cisco TMS Portal, go to **Administrative Tools > Configuration > Provisioning Extension Settings > Collaboration Meeting Room**.
2. Set **Allow Active Meeting Manager** to *No*.

Managing Logs and Reporting Data

TMS Logging for Conductor Failover

If the primary TelePresence Conductor in a cluster goes offline for any reason, the TMS will transfer to a clustered peer node. This is subject to previous configuration in Cisco TMS, as described in Configuring TMS Support for Two-Node Conductor Clusters, page 54).

Cisco TMS records all such transfers and associated messages in the **Conductorfailover-liveservice** log. The log is activated by default. A log entry is triggered if a packet cannot be delivered to the primary Conductor. And when TMS starts using the primary Conductor again.

Logging for Conductor Resource Usage

TelePresence Conductor collects resource usage data based on a set of predefined events, which trigger a log record when they occur. Up to 10 GB of log entries can be stored and be available for download. You can use a third-party tool such as Microsoft Excel to analyze the entries. The log includes information designed to help you determine everyday bridge utilization and hourly usage.

Conductor also writes a log record for every bridge at midnight each day. This ensures that unused bridges are also recorded in the log (as 0% utilization).

Logging is automatically enabled in Conductor.

To download the log:

In Conductor, go to **Maintenance** > **Diagnostics** > **Usage report**. JSON, CSV, or XML formats are available.

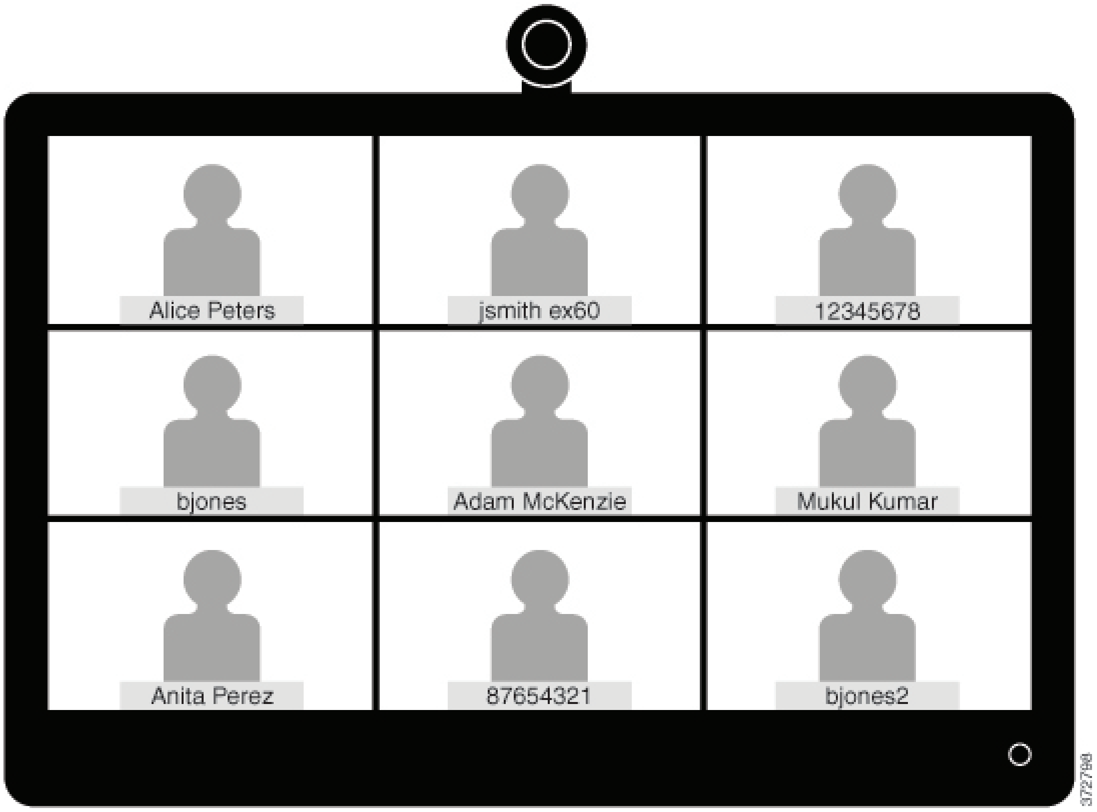
More Information

See the Conductor online help or *Cisco TelePresence Management Suite Administrator Guide* on the TMS Maintain and Operate Guides page.

Appendix 1: Provisioning Display Names Across the Solution

Display names are used across endpoints such as TelePresence to identify a user to other participants. The preferred format is the user's first name and last name (for example *Alice Peters*) or the name of the conference room where the endpoint is installed (for example *MDR21-3-#120* for room 120 on floor 3 of building 21 in Madrid).

Figure 13 Display Names Example



If no display name is explicitly provisioned the system chooses one based on the endpoint's SIP URI or device number. The name will reflect how the particular users and rooms have been provisioned. As a result name information in conferences may be displayed in inconsistent formats, as shown in the example above.

This topic describes how to provision display names so that they appear in a consistent format.

- For information on provisioning endpoints registered to Cisco VCS see Provisioning Display Names for Cisco VCS-Registered Endpoints, page 78.
- If you also have Unified CM-registered endpoints in your network, see Provisioning Display Names for Unified CM-Registered Endpoints, page 80.

Provisioning Display Names for Cisco VCS-Registered Endpoints

Two methods are available to provision display names for Cisco VCS-registered endpoints.

- FindMe templates. Use this method to provision individual users. Each template contains the details for each user, including their Display Name.
- Direct Manage. Use this method to provision Conference Room endpoints. Each Display Name is individually provisioned for each Conference Room endpoint on the endpoint itself.

TMS-Managed Endpoints

For TMS-managed endpoints, an extra configuration recommendation applies. See Display Name for TMS-Managed Endpoints, page 79 below.

FindMe

FindMe is a Cisco TMSPE feature which allows users to specify which video and audio devices should ring when someone calls their ID. A single ID can be used to reach multiple devices associated with that ID. 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, see *Deploying FindMe* in *Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide*, at Cisco TelePresence Management Suite Provisioning Extension page.

Setting Caller ID Display Names for Cisco VCS FindMe Users

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

Note: If you have large numbers of users we recommend that you import their details using Active Directory or LDAP. Then user display names are imported and set automatically.

Before You Start

Cisco TMSPE must be installed and provisioned. 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*, at Cisco TelePresence Management Suite (TMS) Configuration Guides page.

Process

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **User Settings** pane, click **Edit**. The **User Settings** dialog box opens.
3. In the **Display Name** field, enter the first name and last name of the user. If the user was imported using LDAP, the Display Name is already associated with the user.
4. Click **OK**.

Setting Caller ID Display Names for Conference Rooms

This section describes how to use the Direct Manage method to set Display Names for Conference Rooms.

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the Navigator, choose the conference room you want to update from the pane on the left side of the window.
3. Choose the **Address** of the endpoint you want to configure. This takes you to the user interface of the selected endpoint.
4. Choose **Configuration > System Configuration**, and search for ‘display’ in the search field (left side of window).

5. Enter the Display Name in the **Profile 1 DisplayName** field.

   Note: Steps 4 and 5 may vary depending on the endpoint model.

6. Click **Save**.

Display Name for TMS-Managed Endpoints

This step is recommended for TMS-managed endpoints, to avoid labeling mismatches in Active Meeting Manager (and Conference Control Center).

1. Set the **Name** field in TMS to match the **Display Name** defined for the endpoint.

Provisioning Display Names for Unified CM-Registered Endpoints

This section describes how to update display names in the Cisco Unified CM Administration user interface for Unified CM registered endpoints. It explains how users, devices, and lines are configured so that the names display correctly, and also describes some optional advanced settings for trunks.

Users, Devices and Lines

On the Cisco Unified CM Administration user interface, new users are configured in the **User Management > End User** window. You can create new users or 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 are not 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#**.

Display names are configured on the line that is associated with the device. So the display name is set for a particular device to which that user is associated. For shared lines it is possible to set different display names on each appearance of the line. However we recommend you to use the same display name across all devices—using the user's first name and last name or the conference room name.

Using Bulk Administration

You can use Bulk Administration to set the display names for Unified CM-registered endpoints for large numbers of users.

Before You Start

You must first have users configured and associated to devices. For information on provisioning users, see *Cisco Unified Communications Manager Administration Guide* at Cisco Unified Communications Manager (CallManager) Maintain and Operate Guides page.

Process

1. To export user records, see " *Export User Records*" in *Cisco Unified Communications Manager Administration Guide*, at Cisco Unified Communications Manager (CallManager) Maintain and Operate Guides page.
2. In the resulting CSV file that you download, copy the first name and last name columns into a new CSV file.
3. To upload this CSV file to the appropriate device, see " *Update phones using custom file*" in *Cisco Unified Communications Manager Administration Guide*, at Cisco Unified Communications Manager (CallManager) Maintain and Operate Guides page.

Using Manual Configuration

You can manually configure the display name for a Unified CM-registered device. The device may be a shared conference room device or assigned to a specific user.

Before You Start

You must first have users configured and associated to devices. For information on provisioning users, see *Cisco Unified Communications Manager Administration Guide* at Cisco Unified Communications Manager (CallManager) Maintain and Operate Guides page.

Process

1. Log in to the Cisco Unified CM Administration user interface and choose **Device > Phone** to go to the **Find and List Phone** window.
2. Choose the **Device Name(Line)** for the device you want to configure to get to the **Phone Configuration** window for that device.

3. Choose the line for the device from the **Association** area on the left hand side of the window. This takes you to the **Directory Number Configuration** window.
4. In the **Directory Number Information** area, enter the display name in **Alerting name** and **ASCII Alerting name**. This is used to display the user's name when communicating with devices that are not in the Cisco Unified CM cluster.
5. In the **Line 1 on Device** area, enter the display name in **Display (Caller ID)** and **ASCII Display (Caller ID)**. This will appear on devices which are on the same cluster as the Cisco Unified CM.
6. For TMS-managed endpoints, set the **Description** field for each endpoint to match the display name specified in the previous step for the associated line. TMS uses the **Description** [not the **Display (Caller ID)**] as the label/display name in Active Meeting Manager and the Conference Control Center.
7. For shared lines, to ensure changes appear on all devices, check **Update Shared Device Settings**, and click **Propagate selected**.

   For the display name in the Alerting Name, ASCII Alerting Name, Display (Caller ID) and ASCII Display (Caller ID) fields, we recommend using 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 in shared spaces.
8. Click **Save**.

The changes are automatically propagated and take effect immediately unless the endpoint is on an active call, in which case they take effect immediately after the active call ends.

Optional Settings for all Trunks

The following settings can optionally be configured on the **Trunk Configuration** window for further control over display name behavior:

- In the **Device Information** area, check **Transmit UTF-8 for Calling Party Name** to transmit the ASCII Alerting Name on devices that support UTF-8.
- To hide display names on a per-trunk basis, in the **Inbound Calls** area select *Restricted* from the **Connected Name Presentation** drop-down.
- In the **Caller Information** area, you can set **Caller Name** to override individual device display names.

Cisco Legal Information

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

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: 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)