Video Conferencing & Recording Using Cisco BE6000

Cisco Validated Design Guide

October 2015

Contents

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

Documentation for Cisco Validated Designs

Cisco Preferred Architecture (PA) Design Overview guides help customers and sales teams select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.

Cisco Validated Design (CVD) guides provide detailed steps for deploying the Cisco Preferred Architectures. These guides support planning, design, and implementation of the Preferred Architectures.

Cisco Collaboration Solution Reference Network Design (SRND) guide provides detailed design options for Cisco Collaboration. The SRND should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Comments and Questions

If you would like to comment on a guide or ask questions, please email collab-mm-cvd@external.cisco.com.

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

This Cisco validated design guide should be started after deploying the Unified communications using cisco BE6000 cisco validated design guide.

Use Cases

This guide addresses the following technology use cases:

- **Video Collaboration with Desktop and Multipurpose Room Systems**—Organizations want to reap the budgetary and productivity gains that a remote workforce allows, without compromising the benefits of face-to-face interaction. They need a solution that is fast to deploy and easy to manage from a central location, without replicating costly components at their remote sites.

For more information, see the "Use Cases" section in this guide.

Related PA Guides

Cisco Preferred Architecture for Midmarket Collaboration, Design Overview

Cisco Preferred Architecture for Video, Design Overview

Related CVD Guides

Unified Communications Using Cisco Business Edition 6000 CVD

To view the related CVD guides,
click the titles or visit the following site:
http://www.cisco.com/go/cvd/collaboration

Scope

This guide covers the following areas of technology and products:

- Video call agent
- Desktop video endpoints
- Multipurpose room systems
- Video Conference Bridge
- Video Conference Management Systems
- Video Conference Scheduling Systems
- Video Recording Systems
- Session Initiation Protocol (SIP) signaling

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Collaboration**—1 to 3 years configuring voice devices and video single-screen endpoints, supporting telephony and video applications, and troubleshooting.

Introduction

Businesses around the world are struggling with escalating travel costs. Growing corporate expense accounts reflect the high price of travel, but travel also takes a toll on the health and well being of employees and their families. Often, the only way to solve a difficult problem is to fly an expert to the location to see the issue and discuss it with the people at the site. When an expert cannot see what is being described, the resolution of a complex problem often takes much longer.

Workers at remote sites often feel isolated from their departments because they do not spend enough face time with their peers and they feel disconnected from the decision-making process. This isolation can lead to lower job performance and less job satisfaction from employees who do not work at the organization’s main location.

Hiring process can be very lengthy and costly, especially when candidates are located in other cities or when multiple people are involved in the interview process. Organizations with video conferencing systems in their offices can reduce expenses and time by bringing candidates into the nearest facility and allowing interviews to be conducted both in person and over video.

Technology Use Case

The face-to-face interaction during video collaboration meetings helps to boost information retention, promotes increased attention span, and reduces participant confusion. The nonverbal cues experienced in a visual meeting are sometimes more important than what is actually spoken.

Use Case: Video Collaboration with Desktop and Multipurpose Room Systems

Organizations want to reap the budgetary and productivity gains that a remote workforce allows—without compromising the benefits of face-to-face interaction. They want to allow the flexibility for an employee to work across remote sites while still maintaining the familiar in-person contact of their peers and managers. They also want to enrich the collaboration experience in their meeting rooms, boardrooms, auditoriums and other shared environments. A solution is needed that is fast to deploy and easy to manage from a central location without replicating costly components at their remote sites.

This design guide enables the following capabilities:

- Single cluster centralized design to simplify deployment and management while saving on infrastructure components.
- URI and numeric dialing to allow video-enabled IP phones to call room systems.
- Provisioning the videoconference bridge for the site.
- Conference resource optimization, management and scheduling.
- Instant, Personal and Scheduled Collaboration Meeting Rooms (CMR) Conferences.
- Captures video and presentations for live streaming and video-on-demand (VoD) viewing.

Design Overview

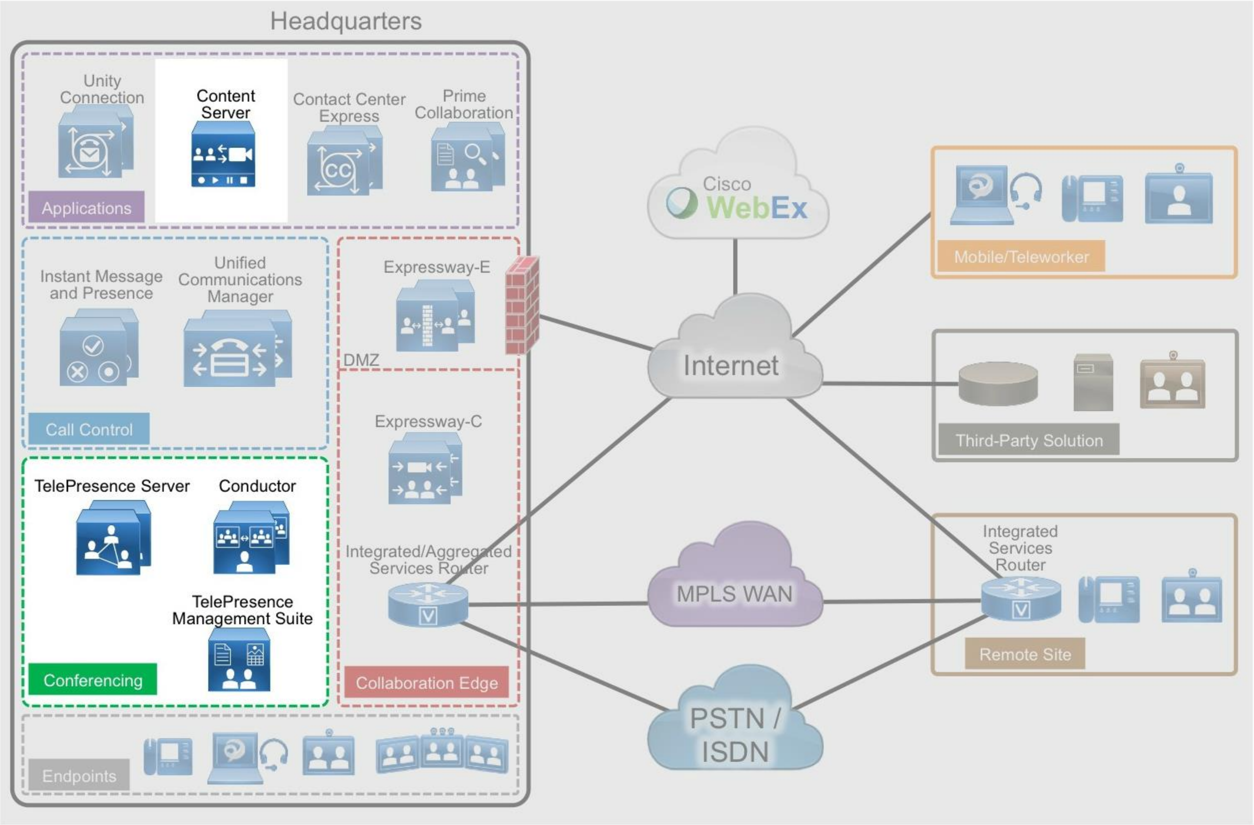
An end-to-end video-collaboration solution incorporates a full suite of endpoints, infrastructure components, and centralized management tools.

Cisco Preferred Architecture

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change.This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

The Cisco Preferred Architecture (PA) delivers capabilities that enable organizations to realize immediate gains in productivity and add value to their current voice deployments.

Figure 1. High level block diagram



Network Considerations

If you already have an IP network in place for voice, your natural next step is to deploy video over IP. Many organizations run video systems in a mixed environment as they move from older systems to newer ones, based on IP. As older systems migrate off of ISDN, significant quality improvements and cost savings will be seen.

Unified communications running over IP offers lower costs, easier management, remote monitoring, and control from across the network. It also provides higher bandwidth for calls, enabling superior audio and video quality while providing tighter integration into the corporate IT mainstream.

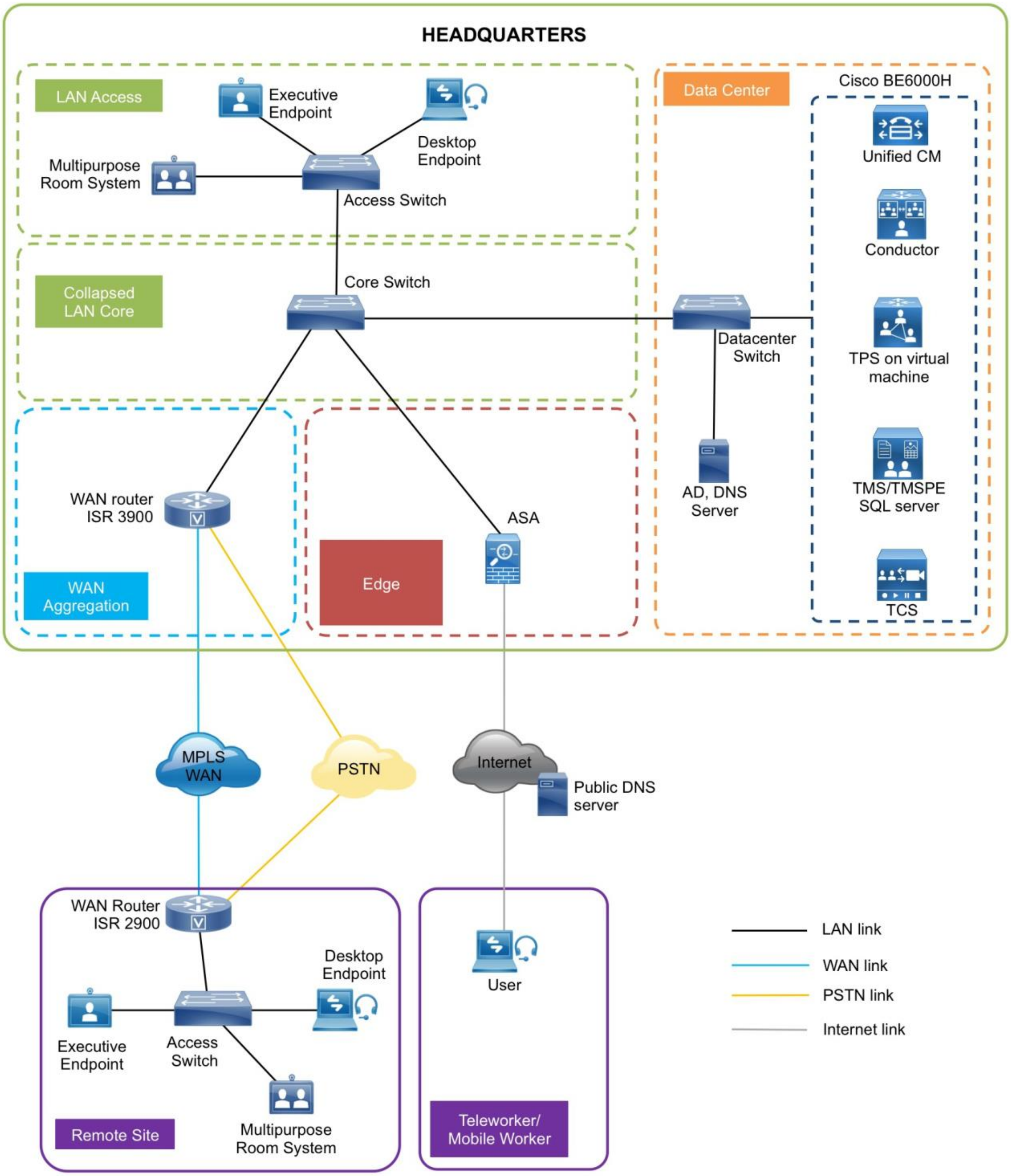
With an IP network, the ongoing costs of running video calls are minimal because you only have to pay for maintenance and technical support. When return on investment (ROI) for the initial deployment is met, any additional costs are essentially free. Because there is no incremental cost involved, employees and managers are more likely to use the technology. As usage goes up, payback times go down, further boosting the ROI.

Solution Details

The Video Conferencing CVD includes the following components:

- Cisco Unified Communications Manager (Unified CM), for call control and SIP endpoint registrations
- Desktop (Cisco 8800 series IP phones, Cisco Jabber and Cisco Desktop Collaboration Experience DX series) and multipurpose (Cisco TelePresence SX 10 and 20 Quick Set) systems for placing and receiving calls
- Cisco TelePresence Server on Virtual Machine, Cisco TelePresence Conductor, Cisco TelePresence Management Suite (TMS) and Cisco TelePresence Management Suite Provisioning Extension (TMSPE) for reservation-less, instant CMR conference (formerly ad-hoc conference), personal CMR conference (formerly rendezvous/static conference) and scheduled CMR conference
- Cisco TelePresence Content server for video and conference recording
- Network Time Protocol (NTP) server for logging consistency

Figure 2. High level network diagram



Cisco Unified Communications Manager

Unified CM serves as the software-based, call-processing component of Cisco Unified Communications. Additional data, voice, and video services, such as unified messaging, rich media conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified Communications Manager open-telephony application program interface (API).

Unified CM is the primary call agent in this CVD. Unified CM supports session initiation protocol (SIP), and the configurations in this document use SIP as the signaling protocol for endpoints.

Cisco Video and TelePresence Endpoints

Cisco video endpoints provide IP video telephony features and functions similar to IP voice telephony, enabling users to make point to point and multipoint video calls. Cisco video endpoints are classified into families based on the features they support, hardware screen size, and environment where the endpoint is deployed.

There are two types of endpoints mentioned in this document:

- Desktop & Mobile Video endpoints—Cisco Jabber software-based clients, such as Cisco Jabber for Windows/Mac/Android/IOS and the Cisco 8800 series IP phones and DX650 endpoints are capable of transmitting video by means of the built-in front-facing camera or a USB attached external camera. The Cisco TelePresence System DX70 and 80 endpoints take the personal desktop solution to a next level of experience with support for content sharing, mobile and remote access.
- Multipurpose endpoints—The Cisco TelePresence SX10 and SX20 Quick Sets are flexible integrators that can turn any display into a powerful Cisco TelePresence system. SX20 Quick Sets are designed for HD video and multiparty conferencing, with the flexibility to accommodate various room sizes.

Cisco TelePresence Server on Virtual Machine

The Cisco TelePresence Server is an innovative software solution enabling high-quality standards-based conferencing for mobile, desktop and immersive endpoints. Compatible with a range of hardware platforms, the TelePresence Server is a versatile, highly scalable solution for midmarket and larger enterprise customers. TelePresence Server on Virtual Machine, which runs on the Cisco Unified Computing System (Cisco UCS) or third party specification-based server platforms, offers a virtualized solution.

Instant, personal and scheduled CMR conferences use TelePresence Server on Virtual Machine to ensure that endpoints can communicate in a single conference at the highest possible bit rates and resolutions, without loss of quality.

Cisco TelePresence Conductor

Cisco TelePresence Conductor software simplifies multiparty video communications, orchestrating the different resources needed for each conference as required. It allows the video network to be configured so that conferences can be easily provisioned, initiated, and accessed. TelePresence Conductor simplifies and enhances conference resource management, making conferences easy to join and administer. It uses knowledge of all available conferencing resources and their capabilities to help ensure dynamic, intelligent conference placement and optimized resource usage. Conductor is a mandatory component when TelePresence Server for Virtual Machine is used for conferencing.

Cisco TelePresence Management Suite

Cisco TelePresence Management Suite (Cisco TMS) enables a variety of scheduling features and management functionality within Cisco Unified Communications including Personal and Scheduled Collaboration Meeting Rooms (CMR) Conferences.

CMRs are reserved virtual spaces that have a set video address. Users can call in to that address at any time to start a meeting. Creation of a CMR requires deployment of TelePresence Conductor with Unified CM, configured with one or more conference bridge pools and Service Preferences. TMS is required to configure Personal and Scheduled CMR Conferences.

Cisco TelePresence Content Server

Cisco TelePresence Content Server adds the functionality of recording videos and conferences and then let them be available as video-on-demand (VoD) for later viewing. There are two scenarios that can be achieved by having the TelePresence Content Server in the solution:

- Dial into the TelePresence Content Server and self record
- Record instant CMR conferences

Cisco TelePresence Content Server is trunked to the Unified CM and a dedicated directory number is used for calls towards the TCS.

Dial Plan

These design uses, single-cluster, centralized call processing. The endpoints use a seven-digit phone number for dialing, which preserves the capability to receive calls from devices that only support only numeric dialing. The numbers are in the following pattern:

- **800xxxx**

For URI dialing the endpoints are assigned the URI in the following pattern:

- **800xxxx@mmcvd.ciscolabs.com**

The domain used in this document is **mmcvd.ciscolabs.com**.

As your solution grows, you may need to acquire a security certificate from a public certification authority. Choose a domain name in this step with a valid Internet domain suffix (.com, .edu etc) to ensure that your system is ready for this requirement.

For instant CMRs, TelePresence Conductor is added as a media resource on the Unified CM.

For personal CMR conferences, TelePresence Conductor is SIP trunked to Unified CM. Personal CMR conferences can have both numbers and URIs. In this document, every user has a dedicated number and

URI configured on the TelePresence Conductor via the TMS. The CMR numbers and URIs used in the following pattern:

- **851xxxx**
- **<user>.cmr@mmcvd.ciscolabs.com e.g. abdey.cmr@mmcvd.ciscolabs.com**

For scheduled CMRs, TelePresence Conductor is SIP trunked to Unified CM. In this document, whenever a user schedules a conference, a randomly generated number is assigned to the scheduled conference for the users to dial in. The scheduled CMR numbers are used in the following pattern:

- **821xxxx**

For recording, TelePresence Content Server is SIP trunked to Unifed CM. For self-video recording the user has to dial a preconfidured DN. For recording an instant CMR conference the user will have to add TCS DN as an additional participant. In this document, this preconfigured DN is in the following pattern:

- **861xxxx**

Deployment Details

This guide is divided into multiple sections: server installations and deploying CMR Premises. Each section has procedures and steps needed to configure the system from the ground up.

For customers who want to deploy both conferencing and recording in their environments, please follow all the procedures in all the process boxes.

For customers who want to deploy only conferencing without the recording capability, please skip the precedures labelled as (recording only).

For customers who want to deploy only recording without the conferencing capability, please follow the procedures labelled as (recording only).

For the installation of Cisco Unified Communications Manager (Unified CM), refer the "Installing the Cisco Unified CM" process in the Installation Guide for Cisco Business Edition 6000.

Easy Access Configuration Sheet

General Networking Parameters		
Item	CVD Configuration	Site Specific Configuration
Domain name	mmcvd.ciscolabs.com	
DNS server	10.106.170.130	
NTP server	10.106.170.130	

Installing TelePresence Server

Easy Access Configuration Sheet

Cisco TelePresence Server Installation Requirements		
Item	CVD Configuration	Site Specific Configuration
TelePresence Server Name	vTS1	
TelePresence Server IP Address	10.106.170.169	
TelePresence Server Subnet Mask	255.255.255.128	
TelePresence Server Default Gateway	10.106.170.129	

Cisco TelePresence Server Configuration Requirements		
Item	CVD Configuration	Site Specific Configuration
User for Conductor to login into TPS	CondAdmin	
User for TMS to login into TPS	TMSAdmin	

PROCESS

This process guides you through installing the TelePresence Server Virtual Machine.

Procedure 1 Configure Cisco Business Edition 6000 connectivity to LAN

The Cisco Business Edition 6000 is connected to a switch in the data center.

Step 1. Using the user account that has ability to make configuration changes, log in to the data center switch.

Step 2. If there is a previous configuration on the switch port where BE6000 is connected, bring the port back to its default state by issuing a no in front of each command.

Step 3. Configure the port as an access port.

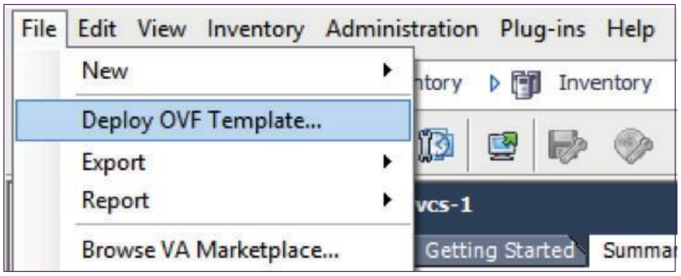
```
interface GigabitEthernet1/14
 description BE6000
 switchport access vlan 20
 switchport host
```

Procedure 2 Deploy OVA to host

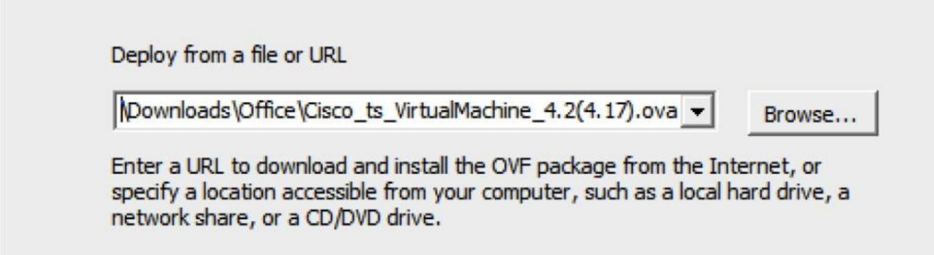
This procedure represents a typical installation. The Deploy OVF Template wizard dynamically changes to reflect host configuration so your steps may vary.

Step 1. Log in to vSphere in order to access the ESXi Host.

Step 2. Select **File > Deploy OVF Template**.



Step 3. Click **Browse**, find the location of the .ova file, click **Open**, and then click **Next**.



Deploy from a file or URL

\Downloads\Office\Cisco_ts_VirtualMachine_4.2(4.17).ova

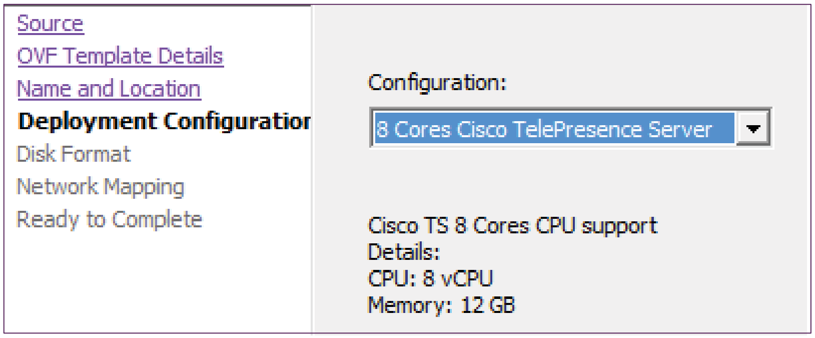
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Step 4. On the OVF Template Details page, click **Next**.

Step 5. If an End User License Agreement page appears, read the EULA, click **Accept** then **Next**.

Step 6. On the Name and Location page, enter **vTS1** and the Inventory Location where the virtual machine will reside.

Step 7. On the Deployment Configuration page, select 8 Cores Cisco TelePresence Server and then click **Next**.



Configuration: 8 Cores Cisco TelePresence Server

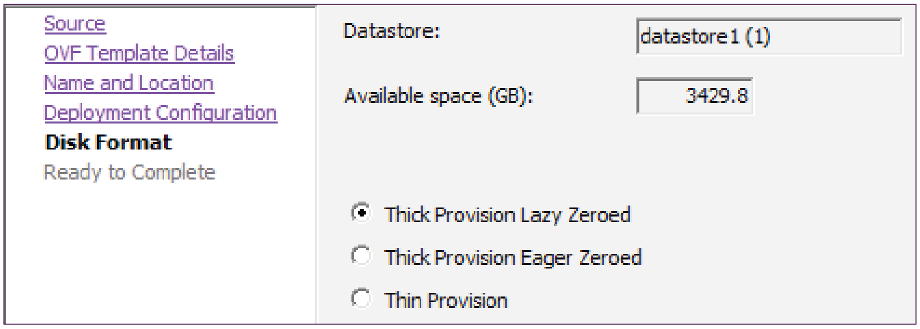
Cisco TS 8 Cores CPU support
Details:
CPU: 8 vCPU
Memory: 12 GB

Step 8. If the Host Cluster page comes, select the host or cluster you want to run the deployed virtual machine, and then click **Next**.

Step 9. If the Resource Pool page comes, select the resource pool with which you want to run the deployed virtual machine, and then click **Next**.

Step 10. If the Storage page comes, select the datastore onto which the TelePresence Server Virtual Machine Guest will be deployed, and then click **Next**.

Step 11. On the Disk Format page, ensure that the default disk format of Thick Provision Lazy Zeroed is selected and then click **Next**.



Datastore: datastore1 (1)

Available space (GB): 3429.8

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

i **Tech Tip**

Because VM performance may degrade during the resizing of a partition, Thin Provision is not recommended.

Step 12. If Network Mapping is listed, configure it and select the network mapping that applies to your infrastructure (the default is VM Network), and then click **Next**.

Step 13. On the Ready to Complete page, confirm your deployment Setting, select **Power on after deployment** and click **Finish**.

The TelePresence Server on Virtual Machine OVA is now deployed as a guest on the VM Host.

Procedure 3 Configure the VM guest

Step 1. Right-click the VM guest and click **'Open Console'**. The VM guest will take some time to boot.

When the TS: prompt appears, login and enter the username **admin** with no password and the TelePresence Server on virtual machine is ready for initial configuration.

Step 2. Configure a static IP address following the format shown in the console and press **Enter**.

```
static 10.106.170.169 255.255.255.128 10.106.170.129
```

You should now be able to access the TelePresence Server via a web browser.

Step 3. Use your browser to navigate to the IP address or host name of the device.

i Tech Tip

The Cisco TelePresence Server on Virtual Machine application must be managed through the Cisco TelePresence Conductor XC4.0 (or later), or a similar system, or through the TelePresence Server API. For more information about the TelePresence Server API, refer to the latest Cisco TelePresence Server API Reference Guide.

Step 4. Click **Log in** and enter the user name **admin** with no password. The Login information page appears.

i Tech Tip

Cisco recommends that you change the admin account to use a password as soon as possible. To do that, on the Login information page, click **Change Password**.

Installing TelePresence Conductor

Easy Access Configuration Sheet

Cisco TelePresence Conductor Installation Requirements		
Items	CVD Configuration	Site Specific Configuration
TelePresence Conductor Name	Cond1	
TelePresence Conductor IP Address	10.106.170.139	
TelePresence Conductor Subnet Mask	255.255.255.128	
TelePresence Conductor Default Gateway	10.106.170.129	
Release Key		
Personal Multiparty License		

Cisco TelePresence Conductor Configuration Requirements		
Item	CVD Configuration	Site Specific Configuration
User for CUCM to login into Conductor	CucmAdmin	
User for TMS (CMR) to login into Conductor	CMRAdmin	
User for TMS (scheduled CMR conferencing) to login into Conductor	TMSAdmin	
Conductor hostname	Cond1	
IP address for Conductor (management)	10.106.170.139	
IP address for Conductor (instant CMR conferences)	10.106.170.143	
IP address for Conductor (scheduled & personal CMR conferences)	10.106.170.144	

PROCESS

1. Deploy OVA to host
2. Configure the VM guest
3. Apply licenses on TelePresence Conductor

Procedure 1 Deploy OVA to host

Step 1. Log in to vSphere to access the ESXi Host.

Step 2. Select **File > Deploy OVF Template**.

Step 3. Select **Source** and browse to the location of the .ova file.

Step 4. Click **Next**.

> i Tech Tip
>
> If the .ova file is already preloaded onto the datastore, you may have to re-enter username and password credentials so that vSphere client can access the web server.

Step 5. On the OVF Template Details page click **Next**.

Step 6. On the End User License Agreement page read the EULA.

Step 7. If you accept the EULA, click **Accept** and then **Next**.

Step 8. On the **Name** and Location page enter **Cond1** as the Name for this TelePresence Conductor VM guest.

Step 9. On the Storage page, select the datastore onto which TelePresence Conductor VM Guest will be deployed, and then click **Next**.

Step 10. On the Disk Format page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.

> i Tech Tip
>
> Because VM performance may degrade during the resizing of a partition, Thin Provision is not recommended.

Step 11. If Network Mapping is listed, configure it and select the network mapping that applies to your infrastructure (the default is VM network), and then click **Next**.

Step 12. On the Ready to Complete page, confirm your deployment settings.

Step 13. Select **Power on after deployment**.

Step 14. Click **Finish**.

The TelePresence Conductor OVA is now deployed as a guest on the VM Host.

Procedure 2 Configure the VM guest

Step 1. Right-click the VM guest and click **Open Console**. The VM guest will take some time to boot.

Step 2. At the login prompt, enter the username **admin**, and the password **TANDBERG**.

Step 3. At the Install Wizard prompt, type **y**, and then press **Enter**.

Step 4. To enter IP information, follow the Install Wizard. Enter the following in the relevant fields. Configure other entries as required.

- Run Install wizard: **y**
- Do you wish to change the system password: **y**
- Password: **[Password]**
- IP Protocol: **IPv4**
- IP Address LAN1: **10.106.170.139**
- Subnet Mask LAN1: **255.255.255.128**
- Default Gateway Address: **10.106.170.129**
- Ethernet Speed: **auto**
- Run ssh daemon: **y**

The configuration is applied and TelePresence Conductor logs you out.

Step 5. Log into TelePresence Conductor as root and then restart the VM guest by typing **restart**.

Step 6. You should now be able to access TelePresence Conductor via a web browser.

Procedure 3 Apply licenses on TelePresence Conductor

For the scenarios covered in this CVD, following are the type of licenses installed on the TelePresence Conductor:

- Release Key
- Personal Multiparty License

i Tech Tip

For additional licensing details, refer the Cisco Preferred Architecture for Midmarket Collaboration, Design Overview.

Step 1. In your browser, enter the correct IP address and log in as admin.

Step 2. Navigate to **Maintenance > Option keys**.

Step 3. On the Option Keys page enter the release key provided in the **Release key** field and then click **Set release key**.

Step 4. On the Options Keys page, under Multiparty Licensing section, set the **Multiparty Licensing for TelePresence Servers** as **Enabled** and click **Save**.

Step 5. For each option key provided, in the **Add option key** field, enter the option key value and then click **Add option**.

Installing TelePresence Management Suite (TMS) and TelePresence Management Suite Provisioning Extension (TMSPE)

Easy Access Configuration Sheet

Cisco TMS Installation Requirements		
Item	CVD Configuration	Site Specific Configuration
TMS Name	TMS on Win Std 2012	
TMS/TMSPE IP Address	10.106.170.153	
TMS/TMSPE Subnet Mask	255.255.255.128	
TMS/TMSPE Default Gateway	10.106.170.129	
Release Key		
IP/ISDN zone name	HQ	
IP/ISDN zone country/region	India	

Cisco TMS Configuration Requirements		
Item	CVD Configuration	Site Specific Configuration
CMR template name	CMR_Template_1	
DN range for CMRs	8510001-8511000	
DN range for scheduled conferences	8211000-8219999	

PROCESS

1. Install Windows Server
2. Install TMS on the Windows Server
3. Install TMSPE on the Windows Server

Installing TMS involves installation of two applications, TMS Core and the TMSPE. Both applications are installed on Windows Server, which is installed as a VM on the BE6000.

This CVD installs the TMS applications on Windows Server 2012 Standard 64 bit Edition with Microsoft SQL Server 2012 64 bit installed on it. TMS stores all its customer data in its SQL database.

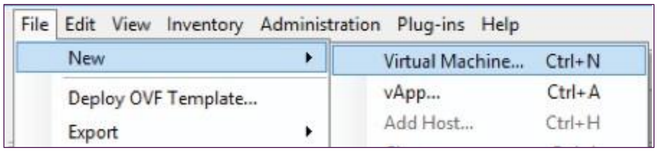
i **Tech Tip**

The SQL Server can also be installed off-box for resiliency.

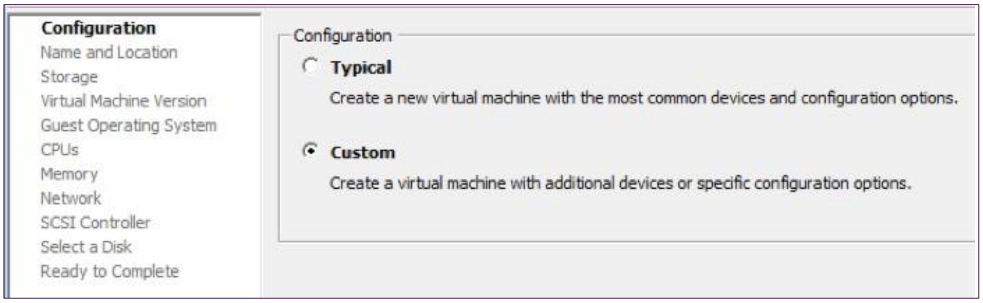
Procedure 1 Install Windows Server

Step 1. Log in to vSphere to access the ESXi Host.

Step 2. Select **File > New > Virtual Machine**.



Step 3. On the Configuration page select **Custom** and click **Next**.



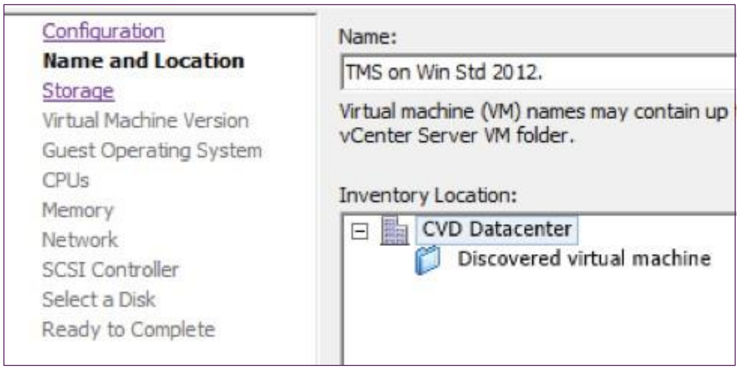
○ Typical

Create a new virtual machine with the most common devices and configuration options.

● Custom

Create a virtual machine with additional devices or specific configuration options.

Step 4. On the Name and Location page, enter **Name** as **TMS on Win Std 2012**, select Inventory Location and click **Next**.



Name:

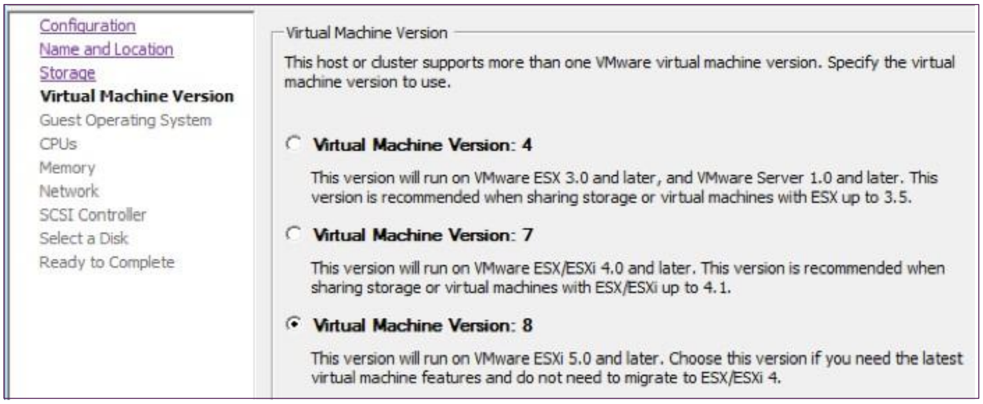
TMS on Win Std 2012.

Virtual machine (VM) names may contain up
vCenter Server VM folder.

Inventory Location:

Step 5. On the Storage page select the datastore and click **Next**.

Step 6. On the Virtual Machine Version page, select **Virtual Machine Version: 8** and click **Next**.



Configuration
Name and Location
Storage
Virtual Machine Version
Guest Operating System
CPUs
Memory
Network
SCSI Controller
Select a Disk
Ready to Complete

Virtual Machine Version

This host or cluster supports more than one VMware virtual machine version. Specify the virtual machine version to use.

○ **Virtual Machine Version: 4**

This version will run on VMware ESX 3.0 and later, and VMware Server 1.0 and later. This version is recommended when sharing storage or virtual machines with ESX up to 3.5.

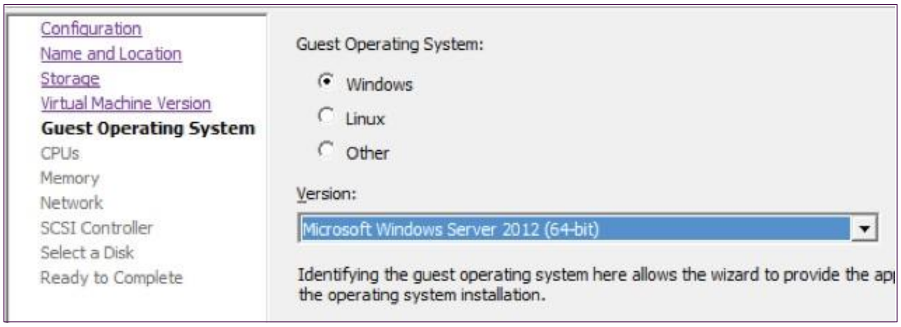
○ **Virtual Machine Version: 7**

This version will run on VMware ESX/ESXi 4.0 and later. This version is recommended when sharing storage or virtual machines with ESX/ESXi up to 4.1.

● **Virtual Machine Version: 8**

This version will run on VMware ESXi 5.0 and later. Choose this version if you need the latest virtual machine features and do not need to migrate to ESX/ESXi 4.

Step 7. On the Guest Operating System page, select **Windows** under Guest Operating System, select **Microsoft Windows Server 2012 (64-bit)** and click **Next**.



Configuration
Name and Location
Storage
Virtual Machine Version
Guest Operating System
CPUs
Memory
Network
SCSI Controller
Select a Disk
Ready to Complete

Guest Operating System:

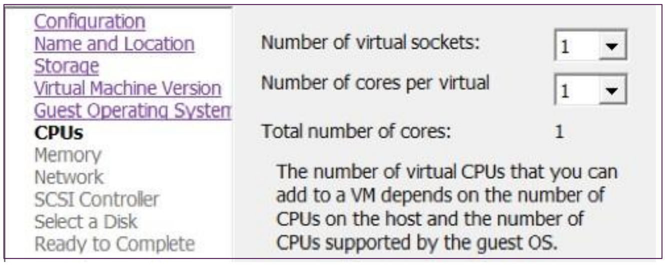
● Windows
○ Linux
○ Other

Version:

Microsoft Windows Server 2012 (64-bit)

Identifying the guest operating system here allows the wizard to provide the ap
the operating system installation.

Step 8. On the CPUs page, select Number of Virtual sockets as 1, select Number of cores per virtual socket as **1** and click **Next**.

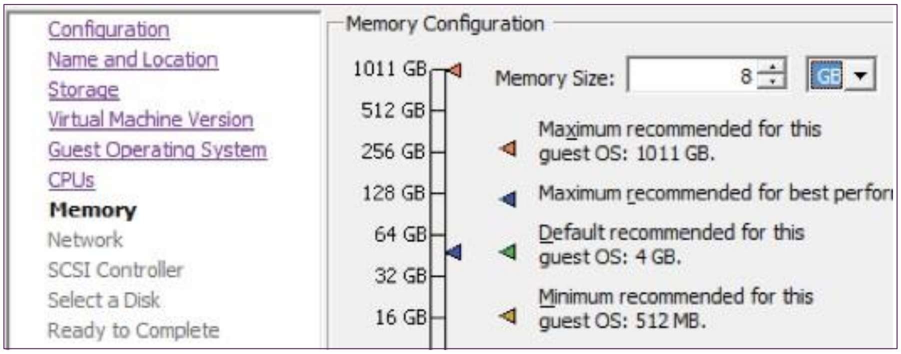


Configuration
Name and Location
Storage
Virtual Machine Version
Guest Operating Systen
CPUs
Memory
Network
SCSI Controller
Select a Disk
Ready to Complete

Number of virtual sockets: 1
Number of cores per virtual 1
Total number of cores: 1

The number of virtual CPUs that you can add to a VM depends on the number of CPUs on the host and the number of CPUs supported by the guest OS.

Step 9. On the Memory page, select Memory Size as **8 GB** and click **Next**.



Memory Configuration

Memory Size: 8 GB

Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best perfor

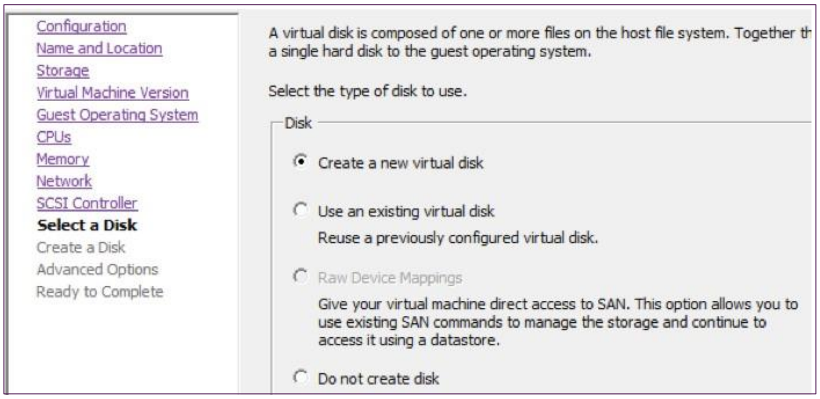
Default recommended for this guest OS: 4 GB.

Minimum recommended for this guest OS: 512 MB.

Step 10. On the Network page, select the How many NICs do you want to connect as 1 and click **Next**.

Step 11. On the SCSI Controller page, select the appropriate settings and click **Next**.

Step 12. On the Select a disk page, select **Create a new virtual disk**, click **Next**.



A virtual disk is composed of one or more files on the host file system. Together th
a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

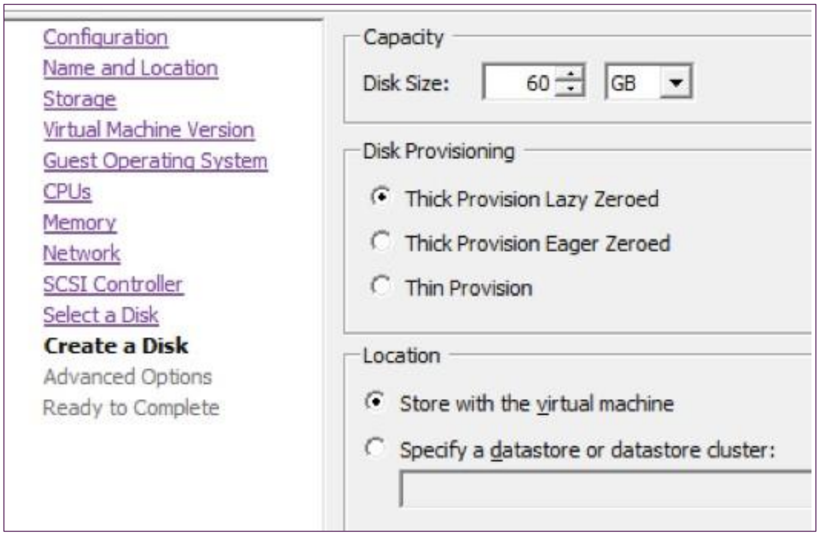
● Create a new virtual disk

○ Use an existing virtual disk
Reuse a previously configured virtual disk.

○ Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

○ Do not create disk

Step 13. On the Create a Disk page, select Disk Size as **60 GB**, Disk Provisioning as **Thick Provision Lazy Zeroed** and click **Next**.



Configuration
Name and Location
Storage
Virtual Machine Version
Guest Operating System
CPUs
Memory
Network
SCSI Controller
Select a Disk
Create a Disk
Advanced Options
Ready to Complete

Capacity

Disk Size: 60 GB

Disk Provisioning

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

Location

● Store with the virtual machine
○ Specify a datastore or datastore cluster:

i Tech Tip

Because VM performance may degrade during the resizing of a partition, Thin provision is not recommended.

Step 14. On the Advanced Options page, select appropriate options and click **Next**.

Step 15. On the Ready to Complete page, confirm your deployment settings and click **Finish**.

Step 16. Once the VM is created, right click on the newly created VM, select Power and click **Power On**.

Step 17. Install Windows Server 2012 Standard on this newly created VM.

Step 18. To configure the IP information, enter the following in the relevant fields. Configure other entries as required.

- IP address—**10.106.170.153**
- Subnet mask—**255.255.255.128**
- Default gateway—**10.106.170.129**
- DNS server—**10.106.170.130**

Step 19. Complete all critical windows update, close all open applications and disable virus-scanning software and other software that may prevent an installation from completing.

Tech Tip

Depending on windows components needing to be added, you may me prompted to reboot the server more than once during the installation. The installer automatically resumes after the server boots.

Step 20. Install SQL Server 2012 on the Windows Server.

Procedure 2 Install TMS on the Windows Server

For the scenarios covered in this CVD, following are the type of licenses installed on the TMS:

- Release Key

Tech Tip

For additional licensing details, refer the Cisco Preferred Architecture for Midmarket Collaboration, Design Overview.

Step 1. Download the Cisco TMS. zip file from cisco.com.

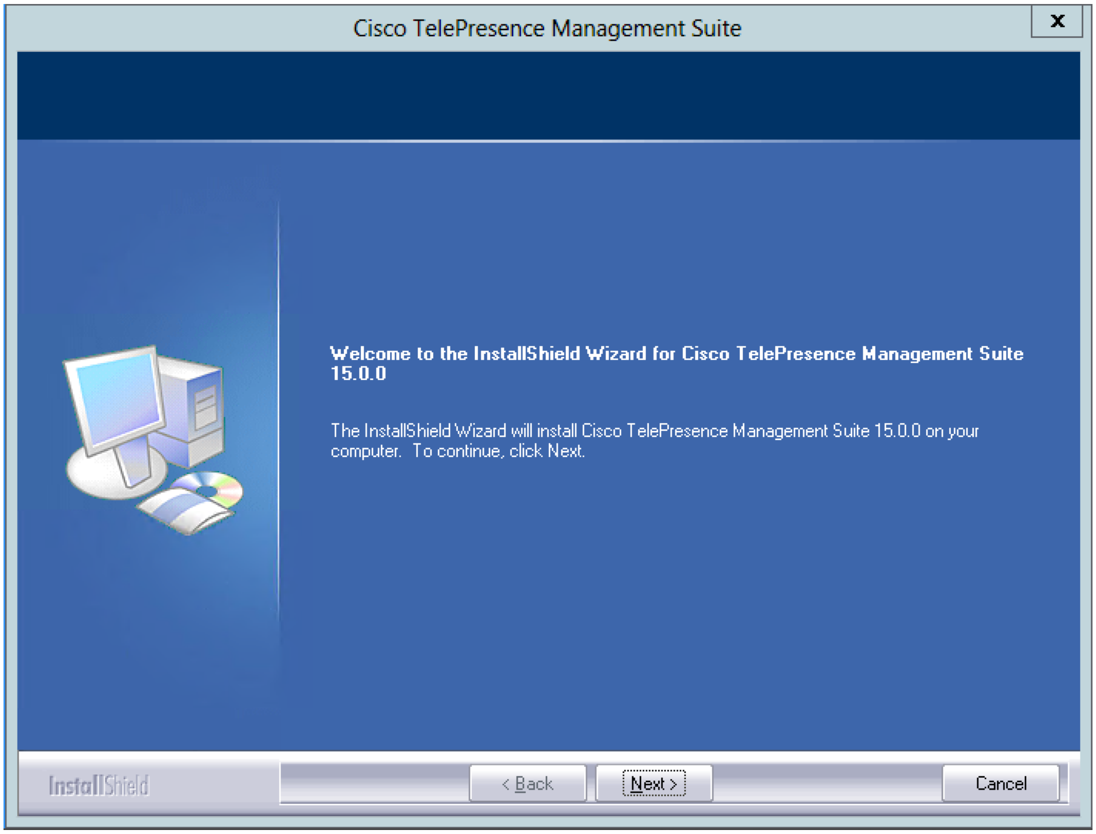
Step 2. Extract the .zip file.

Step 3. Run the Cisco TMS executable as administrator.

The installer now checks the hardware and software configuration of the server. A warning or error message may be displayed depending on your server's configuration. Follow the prompts and install any missing Windows server components.

Step 4. Click **Yes** to continue.

Step 5. On the welcome screen, click **Next**.

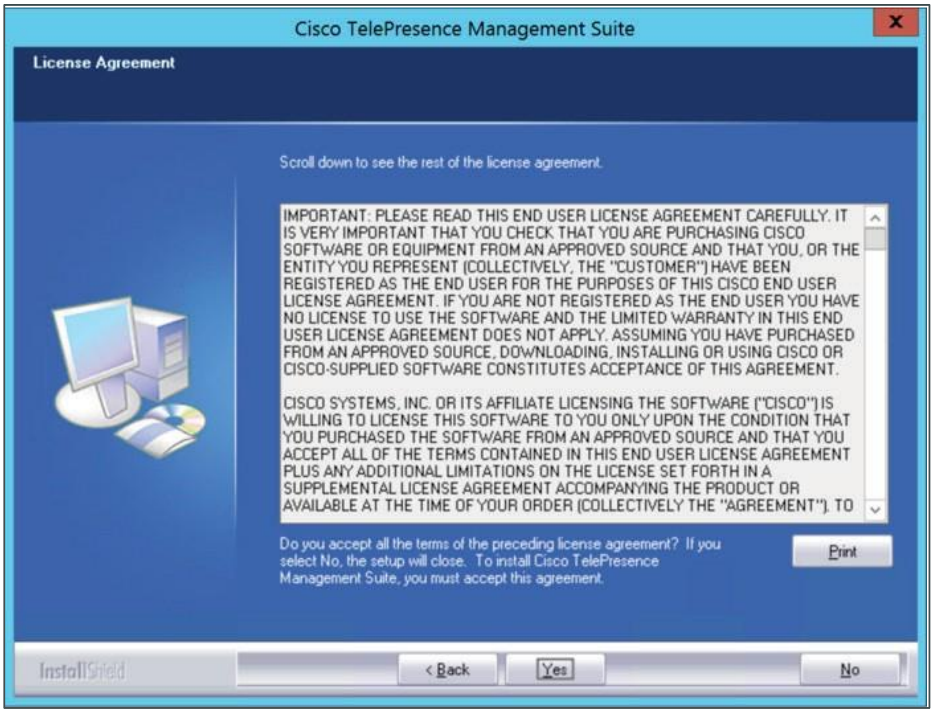


Cisco TelePresence Management Suite

Welcome to the InstallShield Wizard for Cisco TelePresence Management Suite 15.0.0

The InstallShield Wizard will install Cisco TelePresence Management Suite 15.0.0 on your computer. To continue, click Next.

Step 6. On the License Agreement page, click **Yes**.



Cisco TelePresence Management Suite

License Agreement

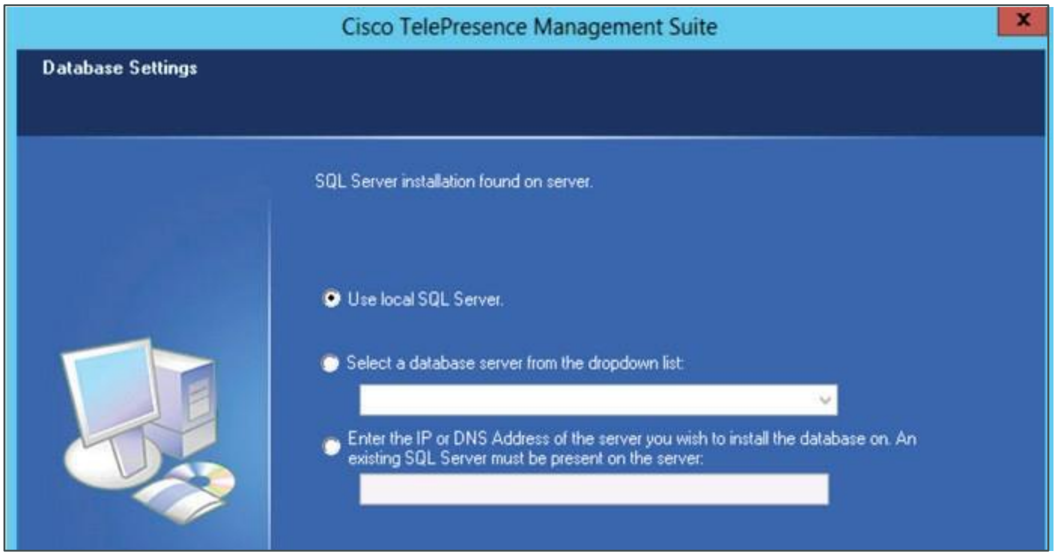
Scroll down to see the rest of the license agreement.

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS AFFILIATE LICENSING THE SOFTWARE ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO

Do you accept all the terms of the preceding license agreement? If you select No, the setup will close. To install Cisco TelePresence Management Suite, you must accept this agreement.

Step 7. On the database setting page, select Use **Local SQL Server**, enter the username, password to allow the installer to create a new database and click **Next**.



Cisco TelePresence Management Suite

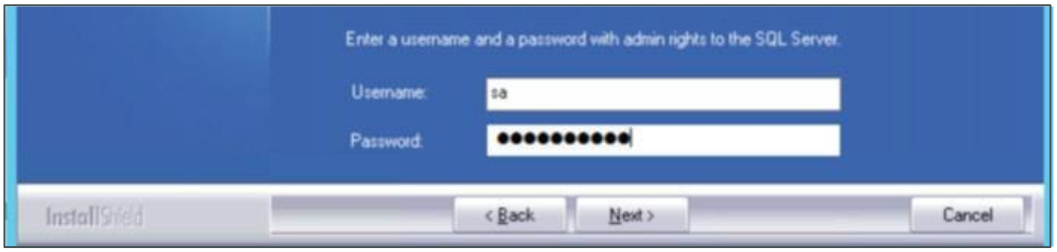
Database Settings

SQL Server installation found on server.

● Use local SQL Server.

○ Select a database server from the dropdown list:

○ Enter the IP or DNS Address of the server you wish to install the database on. An existing SQL Server must be present on the server:



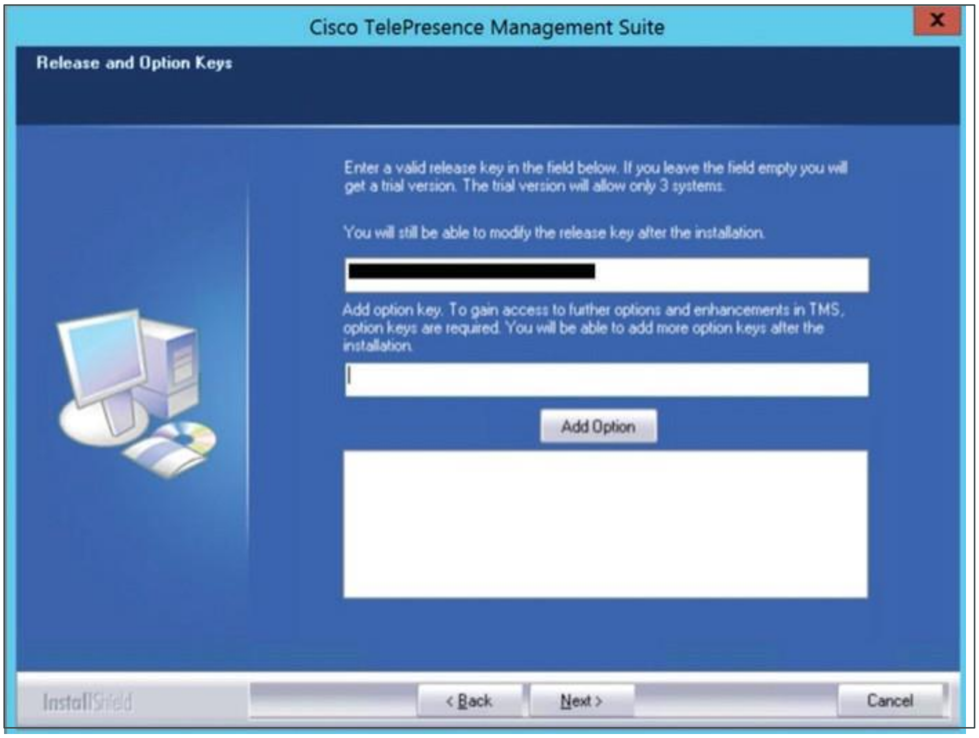
Enter a username and a password with admin rights to the SQL Server.

Username: sa

Password: ●●●●●●●●●●●

i	Tech Tip
The SQL Server can also be installed off-box for resiliency.	

Step 8. On **Release** and **Option Keys** page, enter the release key and click **Next**.



Cisco TelePresence Management Suite

Release and Option Keys

Enter a valid release key in the field below. If you leave the field empty you will get a trial version. The trial version will allow only 3 systems.

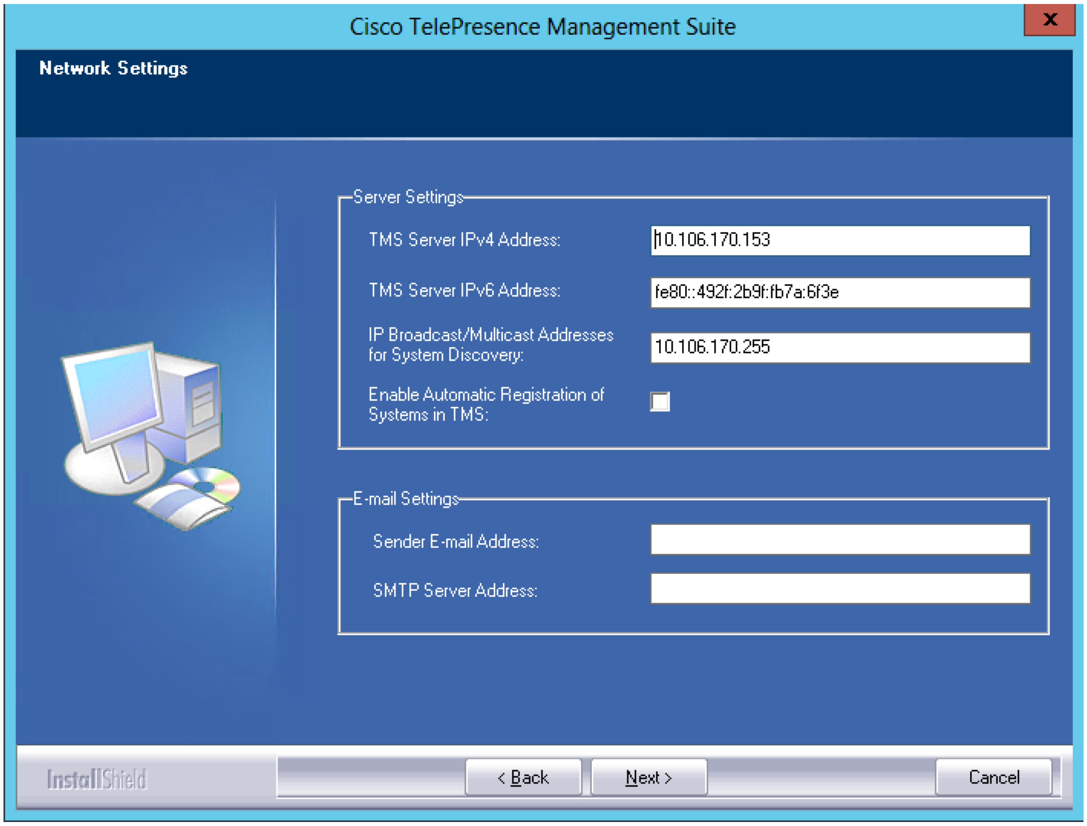
You will still be able to modify the release key after the installation.

[redacted]

Add option key. To gain access to further options and enhancements in TMS, option keys are required. You will be able to add more option keys after the installation.

Step 9. On the **Network** and **Settings** page, enter the following:

- TMS Server IPv4 Address—**10.106.170.153**
- IP Broadcast/Multicast Addresses for system discovery—**10.106.170.255**



Cisco TelePresence Management Suite

Network Settings

Server Settings

TMS Server IPv4 Address: 10.106.170.153

TMS Server IPv6 Address: fe80::492f:2b9f:fb7a:6f3e

IP Broadcast/Multicast Addresses for System Discovery: 10.106.170.255

Enable Automatic Registration of Systems in TMS: □

E-mail Settings

Sender E-mail Address:

SMTP Server Address:

Step 10. Click **Next**.

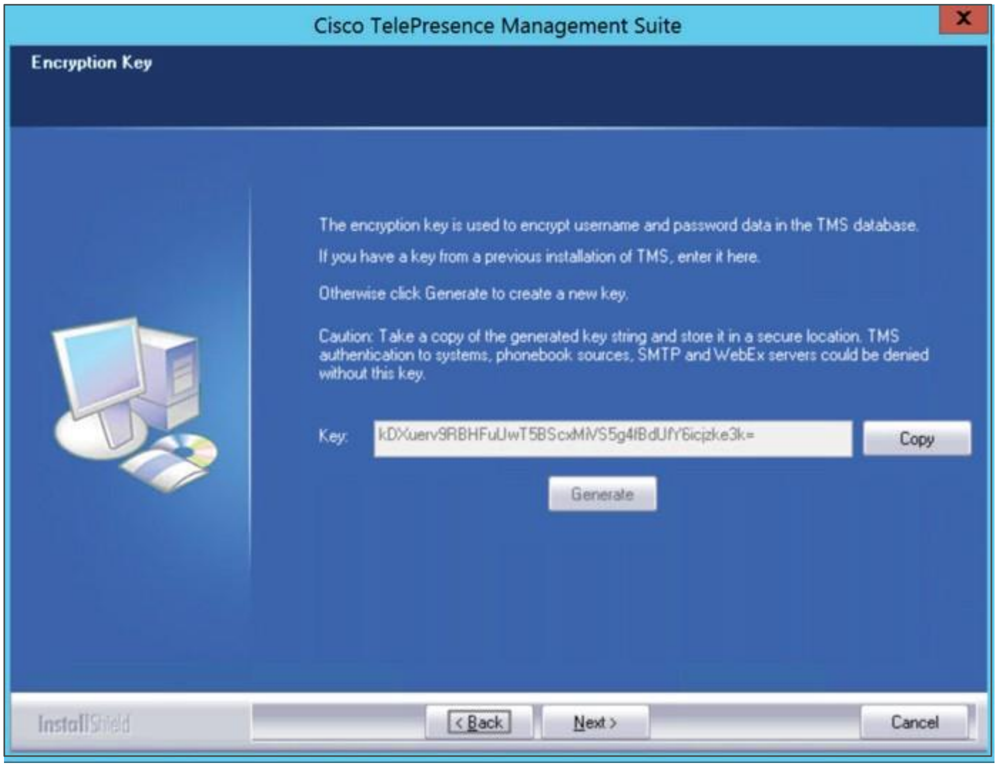
Step 11. On the **IP/ISDN** Zone page, enter the following:

- Name—**HQ**
- Country/Region—**India**

Step 12. Click **Next**.

Step 13. On the **Folder Settings** page, specify the TMS installation path and click **Next**.

Step 14. On the **Encryption Key** page, click **Generate** to generate the new encryption key and click **Copy**.



Cisco TelePresence Management Suite

Encryption Key

The encryption key is used to encrypt username and password data in the TMS database.

If you have a key from a previous installation of TMS, enter it here.

Otherwise click Generate to create a new key.

Caution: Take a copy of the generated key string and store it in a secure location. TMS authentication to systems, phonebook sources, SMTP and WebEx servers could be denied without this key.

Key: kDXuerv9RBHFuUwT5BScxMiVS5g4fBdUfY6icjzke3k=

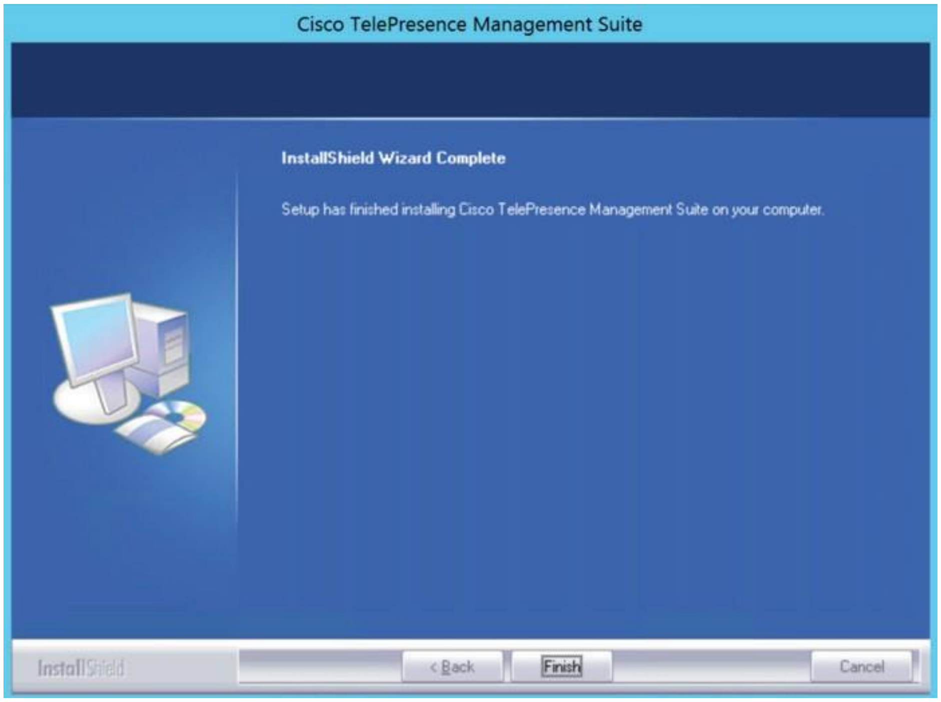
Step 15. Click **Next**.

Step 16. On the **Start Copying Files** page, verify all the settings.

Step 17. Click **Next**.

Step 18. On the **HTTPS for the TMS Website** page, click **Create** to generate a self-signed certificate and click ok.

Step 19. Click **Finish**.



Cisco TelePresence Management Suite

InstallShield Wizard Complete

Setup has finished installing Cisco TelePresence Management Suite on your computer.

The setup wizard is complete.

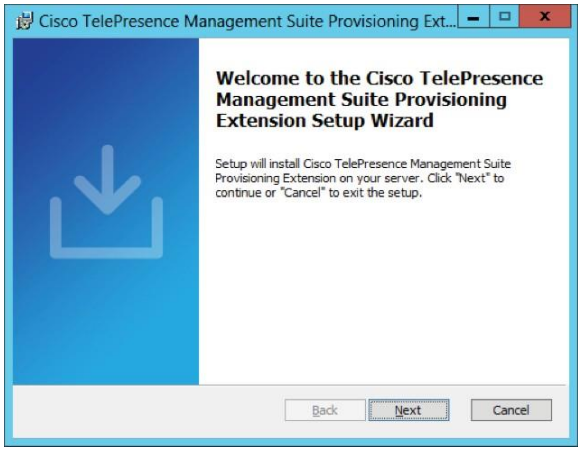
Procedure 3 Install TMSPE on the Windows Server

Step 1. Complete all critical windows update, close all open applications and disable virus-scanning software and other software that may prevent an installation from completing.

Step 2. Make sure that SQL browser service is running and java version 7 is installed (java version 8 is not supported).

Step 3. Extract the TMSPE installer from the zip archive to the TMS server.

Step 4. Run the TMSPE installer as **administrator**.



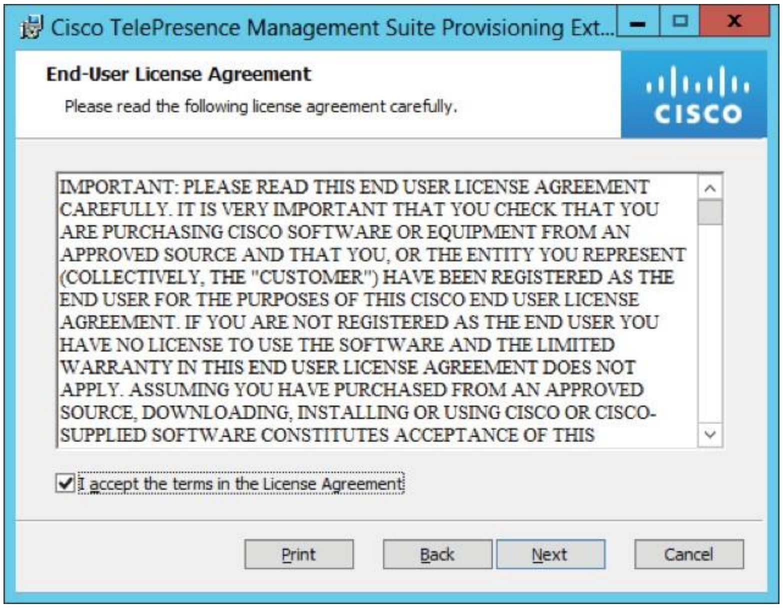
Cisco TelePresence Management Suite Provisioning Ext...

Welcome to the Cisco TelePresence Management Suite Provisioning Extension Setup Wizard

Setup will install Cisco TelePresence Management Suite Provisioning Extension on your server. Click "Next" to continue or "Cancel" to exit the setup.

Step 5. Click **Next**.

Step 6. On the **End-User License Agreement** page, select the **I agree the terms in the License Agreement** checkbox and click **Next**.



Cisco TelePresence Management Suite Provisioning Ext...

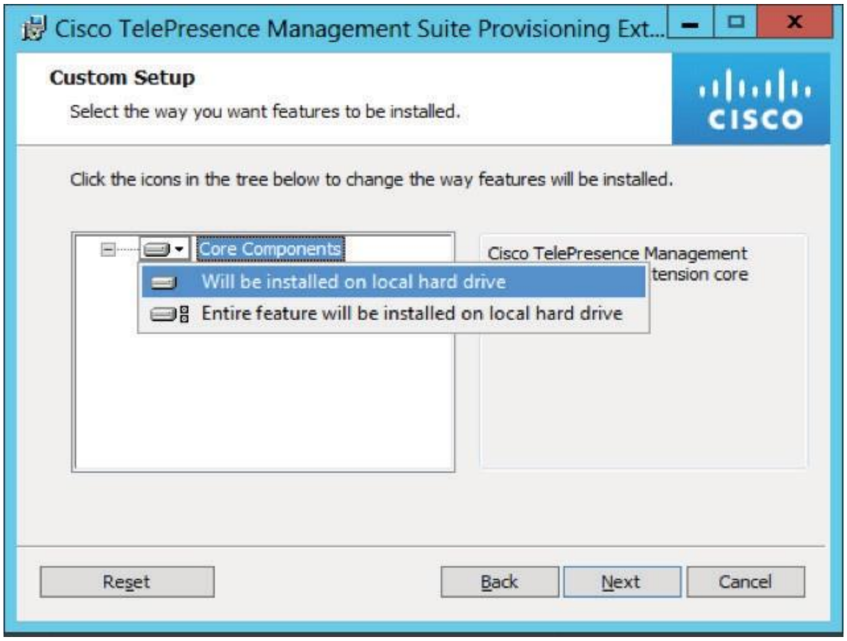
End-User License Agreement

Please read the following license agreement carefully.

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS

☑ I accept the terms in the License Agreement

Step 7. On the **Custom Setup** page, click on the component icons and select the **Will be installed on local hard drive** for all the components and click **Next**.



Cisco TelePresence Management Suite Provisioning Ext...

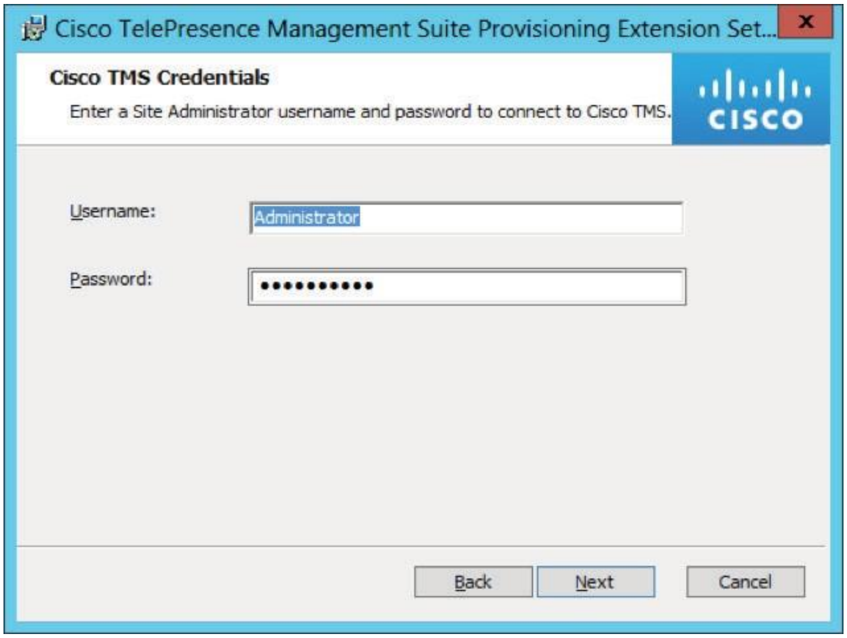
Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

Core Components
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Cisco TelePresence Management
tension core
Reset
Back
Next
Cancel

Step 8. On the **TMS Credentials** page, enter the TMS Admin credentials and click **Next**.



Cisco TelePresence Management Suite Provisioning Extension Set...

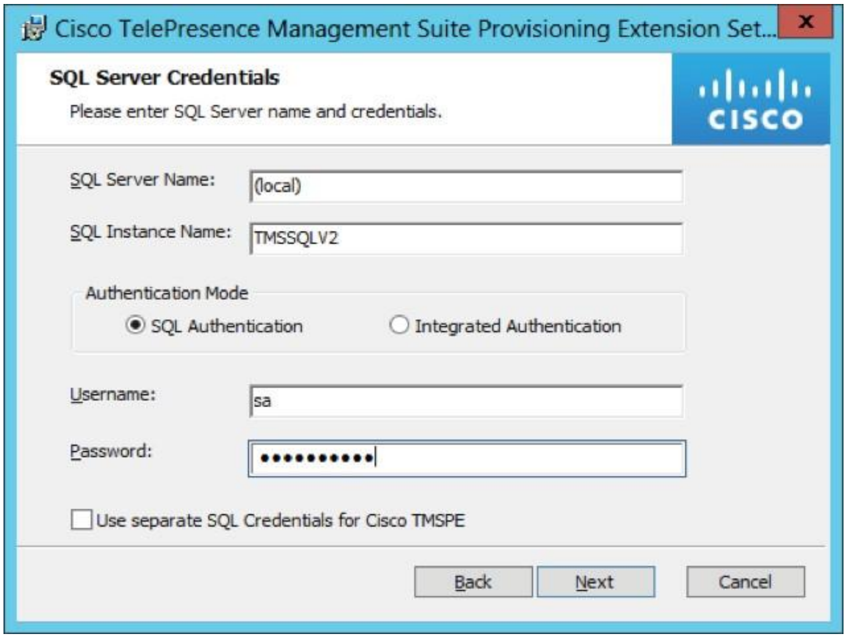
Cisco TMS Credentials

Enter a Site Administrator username and password to connect to Cisco TMS.

Username: Administrator

Password: •••••••••••

Step 9. On the **SQL Server Credentials** page, enter the SQL Server information and click **Next**.



Cisco TelePresence Management Suite Provisioning Extension Set...

SQL Server Credentials

Please enter SQL Server name and credentials.

SQL Server Name: (local)

SQL Instance Name: TMSSQLV2

Authentication Mode

● SQL Authentication ○ Integrated Authentication

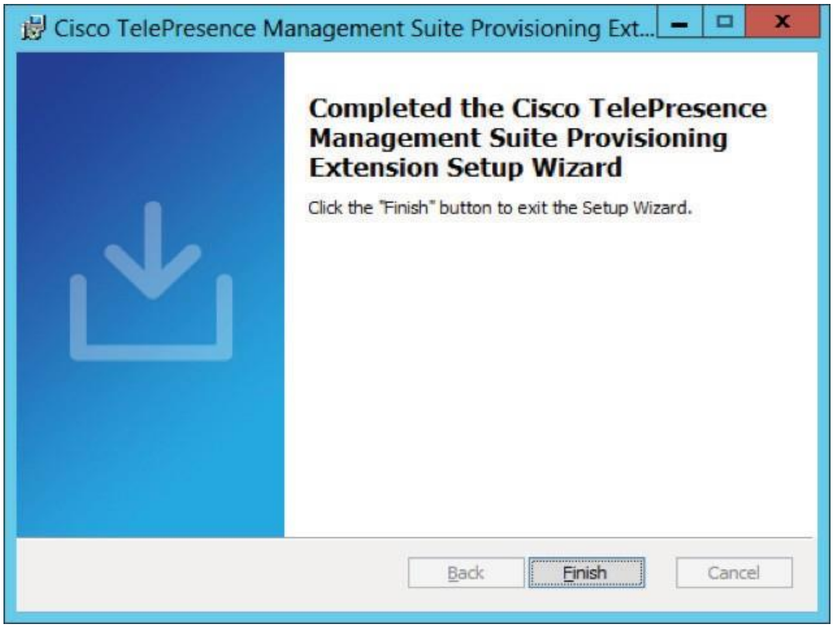
Username: sa

Password: ••••••••••

□ Use separate SQL Credentials for Cisco TMSPE

Step 10. On **Ready to install** page, click **Install**.

Step 11. After the installation is done, click on the **Finish** button to complete the setup wizard.



Cisco TelePresence Management Suite Provisioning Ext...

Completed the Cisco TelePresence Management Suite Provisioning Extension Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

The setup wizard is complete.

i Tech Tip

Please refer the latest "Cisco TelePresence Management Suite Installation and Upgrade Guide" for more installation guidelines.

Installing Cisco TelePresence Content Server

Easy Access Configuration Sheet

Cisco TCS Installation Requirements		
Item	CVD Configuration	Site Specific Configuration
TCS Name	TCS1	
TCS IP Address	10.106.170.195	
TCS Subnet Mask	255.255.255.128	
TCS Default Gateway	10.106.170.129	
Virtual Serial No		
Release Key		
Recording Key		
Live Key		

Cisco TelePresence Conductor Configuration Requirements		
Item	CVD Configuration	Site Specific Configuration
Recording Alias	8610002@mmcvd.ciscolabs.com	

PROCESS

1. Deploy OVA to host (recording only)
2. Install Windows Server 2008 Standard R2 SP1 (recording only)
3. Install IIS on the Windows Server (recording only)
4. Install Window Media Services on the Windows Server (recording only)
5. Install Windows Server Features on the Windows Server (recording only)
6. Install TCS on the Windows Server (recording only)

Procedure 1 Deploy OVA to host (recording only)

Step 1. Log in to vSphere to access the ESXi Host.

Step 2. Select **File > Deploy OVF Template**.

Step 3. Select **Source** and browse to the location of the .ova file.

Step 4. Click **Next**.

Step 5. On the OVF Template Details page click **Next**.

Step 6. On the **Name** and Location page enter **TCS1** as the Name for this TelePresence Content Server VM guest.

Step 7. On the Disk Format page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.

i Tech Tip

Because VM performance may degrade during the resizing of a partition, Thin Provision is not recommended.

Step 8. On the Ready to Complete page, confirm your deployment settings, select **Power on after deployment** and click **Finish**.

Step 9. The TelePresence Content Server OVA is now deployed as a guest on the VM Host.

Procedure 2 Install Windows Server 2008 Standard R2 SP1 (recording only)

Step 1. Install Windows Server 2008 Standard R2 Service Pack 1 in the new VM created in the previous procedure.

Step 2. Create two partitions on the host while installing Windows:

- C: for program files with a minimum of 100 GB space
- E: for media files with the remainder of available space

Step 3. Follow the prompts to complete the Windows Server installation.

Step 4. Install VMware Tools.

Step 5. To configure the IP information, enter the following in the relevant fields:

- IP address – **10.106.170.195**
- Subnet mask – **255.255.255.128**
- Default gateway – **10.106.170.129**
- DNS server – **10.106.170.130**

Step 6. Complete all critical windows update, close all open applications and disable virus-scanning software and other software that may prevent an installation from completing.

i	Tech Tip
	Depending on windows components needing to be added, you may me prompted to reboot the server more than once during the installation. The installer automatically resumes after the server boots.

Windows is installed.

Procedure 3 Install IIS on the Windows Server (recording only)

Step 1. On the VM host, navigate to **Server Manager > Roles > Add Roles**. Click the **Web Server (IIS)** check box and click **Next**.

Step 2. In the Select Role Services window, select all the roles services. Click **Next.**

Step 3. Click **Install** to complete the IIS installation.

Procedure 4 Install Window Media Services on the Windows Server (recording only)

Step 1. Download Windows Media Services (WMS) from http://www.microsoft.com.

Step 2. Install the update.

Step 3. Navigate to **Server Manager > Roles > Add Roles**. Select the Streaming Media Services check box and click **Next**.

Step 4. In the Select Role Services window, select the three **Role Services** check boxes and click **Next**. A pop-up window appears for installing the dependent services. Click **OK** to install the dependent services.

Step 5. In the Data Transfer Protocols window, select the **Real Time Streaming Protocol (RTSP)** check box and click **Next**.

Step 6. Click **Install** to complete the WMS installation.

Windows Media Services are Installed.

Procedure 5 Install Windows Server Features on the Windows Server (recording only)

Step 1. Navigate to **Server Manager > Features > Add Features**.

Step 2. In the Select Features window, select the **Windows Server Backup Features**, **Windows Server Back**, and **Command-line** Tools check boxes and click **Next**.

Step 3. Click Install to install the Backup Features.

Step 4. Navigate to **Server Manager > Features > Add Features**.

Step 5. In the Select Features window, click the **Desktop Experience** check box and click **Next.**

Step 6. Click Install to install the Desktop Experience.

Step 7. A pop-up appears for installing the dependent services. Click **Okay** to install the dependent services.

Step 8. Click **Restart** to restart the system.

Windows server features are installed.

Procedure 6 Install TCS on the Windows Server (recording only)

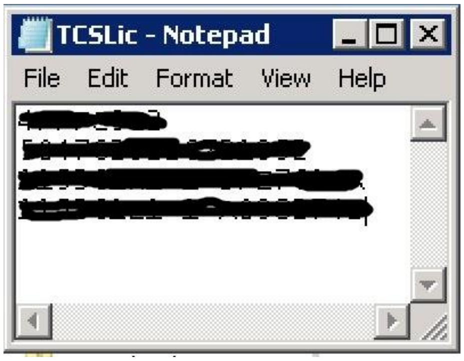
Step 1. Run dotNetFx40_Full_x86_x64.exe package to install .NET.

Step 2. Launch the command prompt and run as an administrator. Go to the location, where the TCS_6.2_BE6K_Package.zip is extracted.

Run GetTCSVirtualSN.exe to generate the virtual serial number (vSN) for your Content Server VM. Copy the virtual serial number.

Step 3. In the TCS_6.2_BE6K_Package.zip extracted directory, create a *TCSLic.txt* file by using the licensing information in this format:

- **Virtual Serial No**
- **Release Key**
- **Recording 1 Key**
- **Live 1 Key**



[redacted]

i	Tech Tip
	In the license text file, make sure that there are no extra spaces before or after the license keys.

Step 4. In the command prompt, run the **PreInstaller.cmd** from the extracted **TCS_6.2_BE6K_Package.zip** directory to configure the Content Server Pre-Installer.

Step 5. Run **S6_2_VM.exe** to install the VM Content Server software on the appliance. Follow the prompts to complete the TCS installation.

Step 6. Run the **PostInstaller.cmd** from the VM Scripts folder in the command prompt to configure the Post-Installer. This will reboot the system.

Cisco TelePresence Content Server is installed.

Configuring Cisco TelePresence Server

PROCESS

Procedure 1 Create a user for Conductor

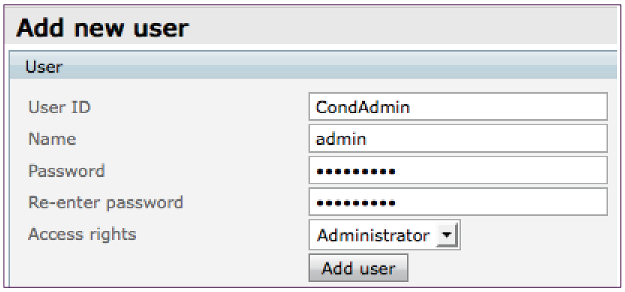
For TelePresence Conductor to communicate with the TelePresence Server, it must use credentials for a user account that has administrator rights. We recommend that you create a dedicated administrator-level user for this task.

Step 1. On the web interface of the virtual TelePresence Server you want to configure, log in as an administrator.

Step 2. Navigate to **User > Add New User**.

Step 3. Enter the following in the relevant fields, configure other entries as required:

- User ID—**CondAdmin**
- Name—**Admin**
- Access rights—**Administrator**



Add new user

User

User ID	CondAdmin
Name	admin
Password	•••••••••
Re-enter password	•••••••••
Access rights	Administrator

Step 4. Click **Add user**.

Step 5. Enable HTTPS by going to **Network > Services** and enter the following value:

- HTTPS checked—**443**

Step 6. Click **Apply changes**.

Procedure 2 Create a user for TMS

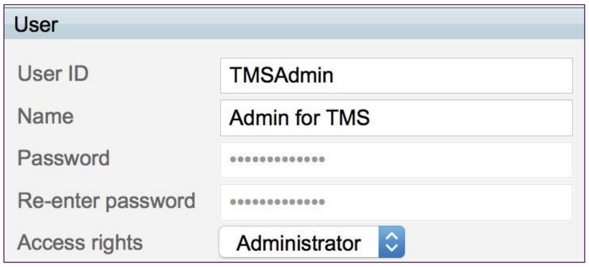
For TMS to communicate with the TelePresence Server, it must use credentials for a user account that has administrator rights. We recommend that you create a dedicated administrator-level user for this task.

Step 1. On the web interface of the virtual TelePresence Server you want to configure, log in as an administrator.

Step 2. Navigate to User > Add New User.

Step 3. Enter the following in the relevant fields, configure other entries as required:

- User ID–**TMSAdmin**
- Name–**Admin for TMS**
- Access rights–**Administrator**



User

User ID	TMSAdmin
Name	Admin for TMS
Password	•••••••••••••
Re-enter password	•••••••••••••
Access rights	Administrator

Step 4. Click Add user.

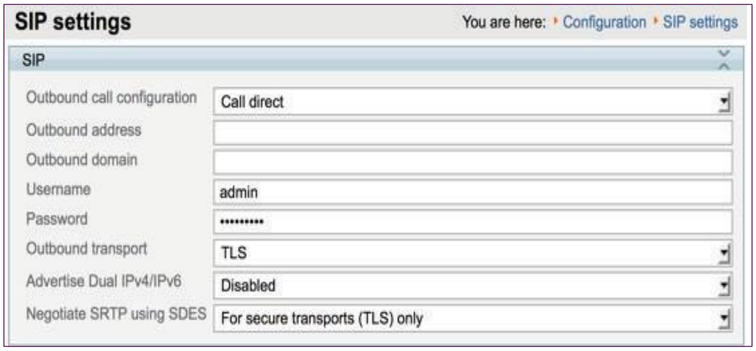
Procedure 3 Configure SIP

The TelePresence Server needs the ability to dial out to devices, for example, when an auto-dialed participant is associated with a template in TelePresence Conductor. To do this, the TelePresence Server needs to know where to direct signaling requests.

Step 1. Go to **Configuration > SIP Settings**.

Step 2. Enter the following values into the relevant fields:

- Outbound call configuration—**Call Direct**
- Outbound address—Leave Blank
- Outbound domain—Leave Blank
- Username—**[username]**
- Password—**[password]**
- Outbound Transport—**TLS**
- Advertise Dual IPv4/IPv6—**Disabled**
- Negotiate SRTP using SDES—**For Secure Transport (TLS) only**



SIP settings

You are here: Configuration ▸ SIP settings

SIP

Outbound call configuration	Call direct
Outbound address	
Outbound domain	
Username	admin
Password	•••••••••
Outbound transport	TLS
Advertise Dual IPv4/IPv6	Disabled
Negotiate SRTP using SDES	For secure transports (TLS) only

Step 3. Click **Apply changes.**

Configuring Cisco TelePresence Conductor

PROCESS

1. Create a user for Unified CM access
2. Create a user for TMS CMR access
3. Create a user for TMS-scheduled conference access
4. Change the system settings
5. Add IP addresses for instant, personal and scheduled CMR conference locations on Conductor
6. Create Service preferences
7. Set up conference bridge pools
8. Add Conference Bridge Pool in Service preference
9. Create a conference template for an instant CMR conference
10. Create a conference template for personal CMR conferences
11. Create a conference template for scheduled CMR conference
12. Create a conference alias for an personal CMR conferences
13. Create a conference alias for an scheduled CMR conference
14. Create locations in Conductor
15. Add locations to conference bridge pools

Procedure 1 Create a user for Unified CM access

For Unified CM to communicate with TelePresence Conductor, you must configure a user with administrator rights on TelePresence Conductor. We recommend that you create a dedicated Read-write user for this task.

Step 1. Log into TelePresence Conductor as a user with administrator rights.

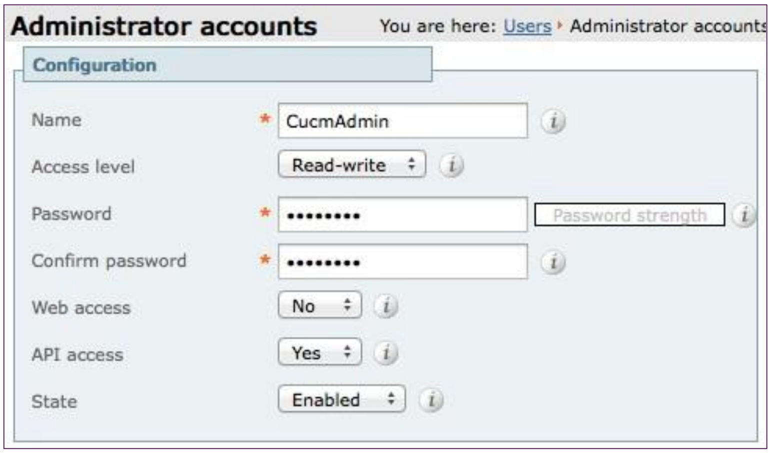
Step 2. Go to **Users > Administrator** accounts.

Step 3. Click **New**.

Step 4. Enter the following in the relevant fields:

- Name—**CucmAdmin**
- Access level—**Read-Write**
- Password—**[Password]**

- Web access–**No**
- API access–**Yes**
- State–**Enabled**



Administrator accounts

You are here: Users ▸ Administrator accounts

Configuration

Name *	CucmAdmin
Access level	Read-write
Password *	••••••••
Confirm password *	••••••••
Web access	No
API access	Yes
State	Enabled

Step 5. Click **Save**.

Procedure 2 Create a user for TMS CMR access

For TMS to communicate with TelePresence Conductor, you must configure a user with administrator rights on TelePresence Conductor. We recommend that you create a dedicated Read-write user for this task.

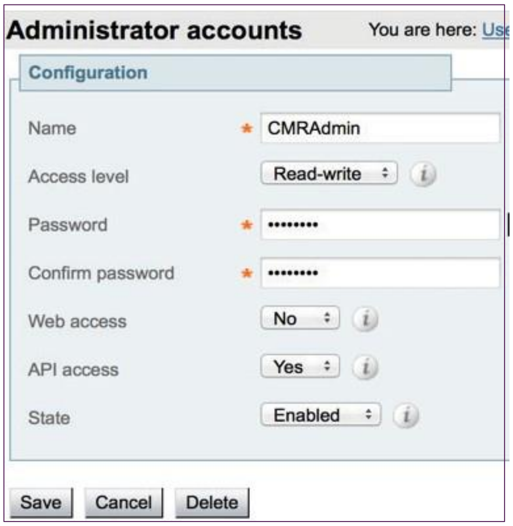
Step 1. Log into TelePresence Conductor as a user with administrator rights.

Step 2. Go to **Users > Administrator accounts.**

Step 3. Click **New**.

Step 4. Enter the following in the relevant fields:

- Name—**CMRAdmin**
- Access level—**Read-Write**
- Password—**[Password]**
- Web access—**No**
- State—**Enabled**



Administrator accounts

You are here: Use

Configuration

Name *	CMRAdmin
Access level	Read-write
Password *	••••••••
Confirm password *	••••••••
Web access	No
API access	Yes
State	Enabled

Step 5. Click **Save**.

Procedure 3 Create a user for TMS-scheduled conference access

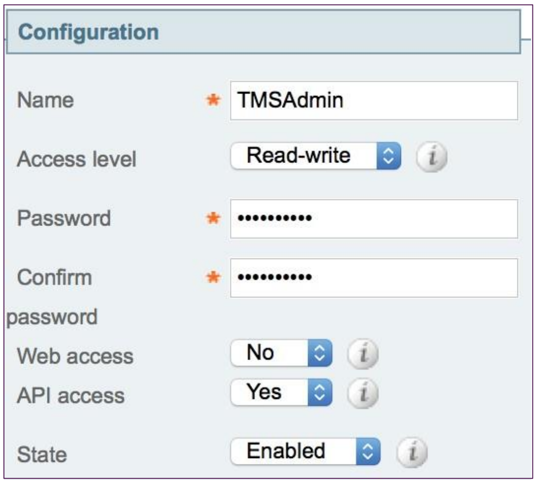
Step 1. Log into TelePresence Conductor as a user with administrator rights.

Step 2. Go to **Users > Administrator** accounts.

Step 3. Click **New**.

Step 4. Enter the following in the relevant fields:

- Name—**TMSAdmin**
- Access level—**Read-Write**
- Password—**[Password]**
- Web access—**No**
- API access—**Yes**
- State—**Enabled**



Configuration

Name	*	TMSAdmin
Access level		Read-write
Password	*	••••••••••
Confirm password	*	••••••••••
Web access		No
API access		Yes
State		Enabled

Step 5. Click **Save**.

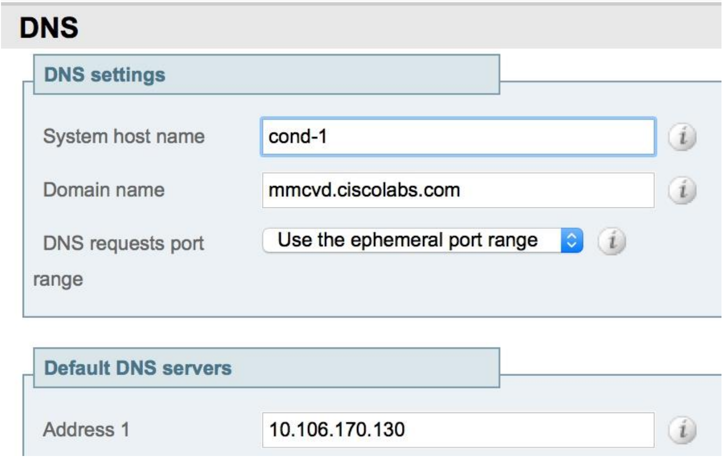
Procedure 4 Change the system settings

Step 1. Navigate to **System > DNS** and enter the following values into the relevant fields:

- System host name—**cond1**
- Domain name—**mmcvd.ciscolabs.com**
- Address 1—**10.106.170.130**

i Tech Tip

The FQDN of TelePresence Conductor will be **cond1.mmcvd.ciscolabs.com**



DNS

DNS settings

System host name: cond-1

Domain name: mmcvd.ciscolabs.com

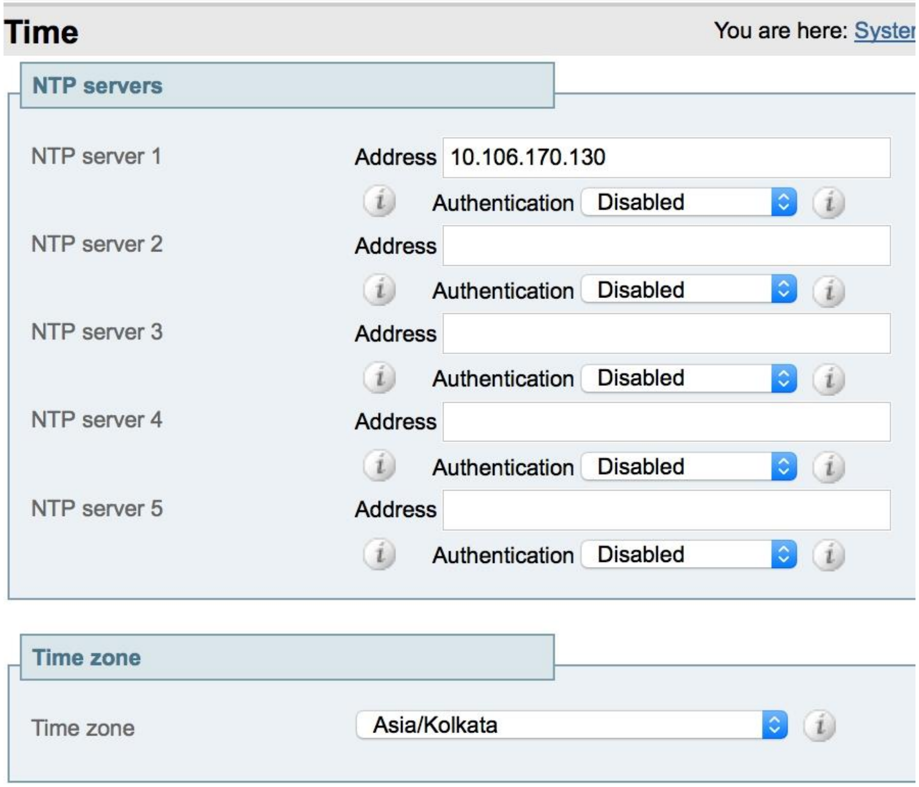
DNS requests port range: Use the ephemeral port range

Default DNS servers

Address 1: 10.106.170.130

Step 2. Click **Save**.

Step 3. Navigate to **System > Time** and set **NTP server 1** to **10.106.170.130**.



Time

You are here: Syster

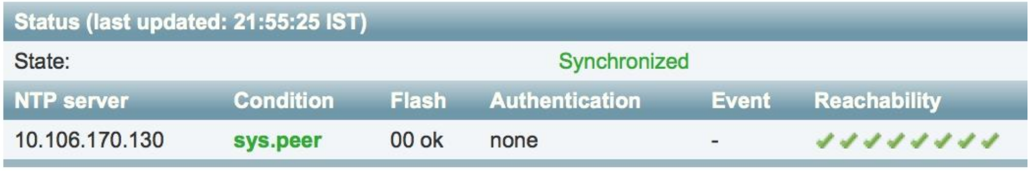
NTP servers

NTP server 1	Address	10.106.170.130
	Authentication	Disabled
NTP server 2	Address	
	Authentication	Disabled
NTP server 3	Address	
	Authentication	Disabled
NTP server 4	Address	
	Authentication	Disabled
NTP server 5	Address	
	Authentication	Disabled

Time zone

Time zone: Asia/Kolkata

Step 4. Ensure that under the Status section, the State is **Synchronized**. Synchronization can take a couple of minutes.



Status (last updated: 21:55:25 IST)

State: Synchronized

NTP server	Condition	Flash	Authentication	Event	Reachability
10.106.170.130	sys.peer	00 ok	none	-	✓✓✓✓✓✓✓✓

Procedure 5 Add IP addresses for instant, personal and scheduled CMR conference locations on Conductor

Step 1. In **System > Network interfaces > IP**, in the Additional addresses for LAN 1 section click **New**.

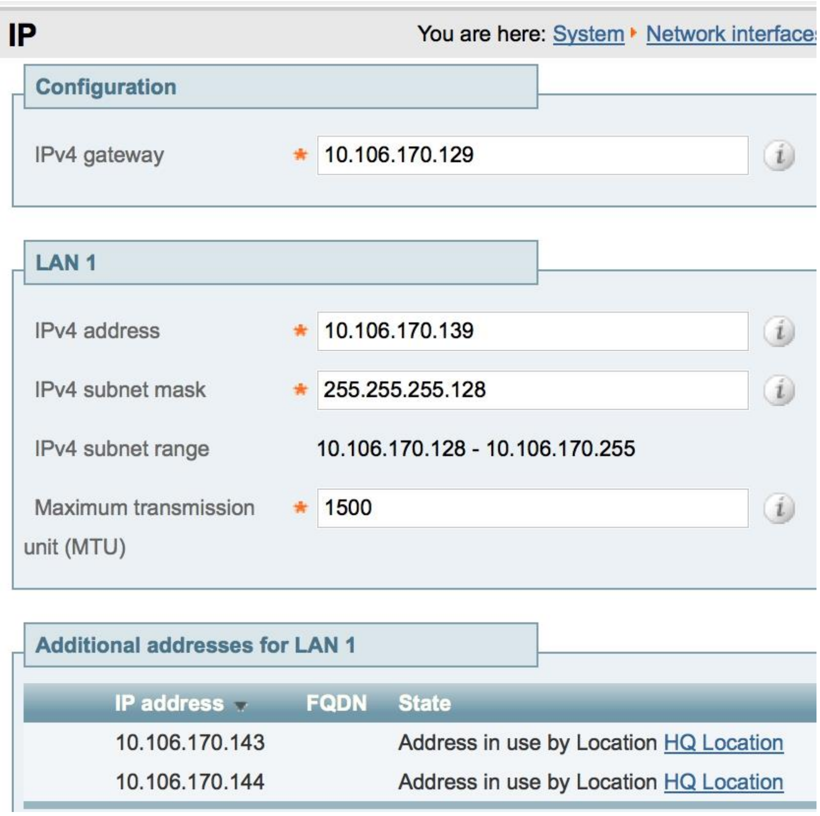
Step 2. Add the IP addresses used for instant CMRs (**10.106.170.143**) and click **Add Address**.

i Tech Tip

These IP addresses must be on the same subnet as the primary TelePresence Conductor IP interface, and they must be reserved for use by this TelePresence Conductor alone.

Step 3. Add the IP addresses used for personal and scheduled CMR conferences (**10.106.170.144**) and click **Add address**.

Step 4. In the Additional addresses for LAN 1 list, verify that the IP addresses were added correctly.



IP

You are here: System ▸ Network interface

Configuration

IPv4 gateway * 10.106.170.129

LAN 1

IPv4 address * 10.106.170.139

IPv4 subnet mask * 255.255.255.128

IPv4 subnet range 10.106.170.128 - 10.106.170.255

Maximum transmission unit (MTU) * 1500

Additional addresses for LAN 1

IP address	FQDN	State
10.106.170.143		Address in use by Location HQ Location
10.106.170.144		Address in use by Location HQ Location

Step 5. Navigate to **Maintenance > Restart** options and click **Restart**. Your network interface changes are applied.

Step 6. Wait for TelePresence Conductor to restart and then verify that the new TelePresence Conductor IP address is active on the network by pinging the IP address from another device.

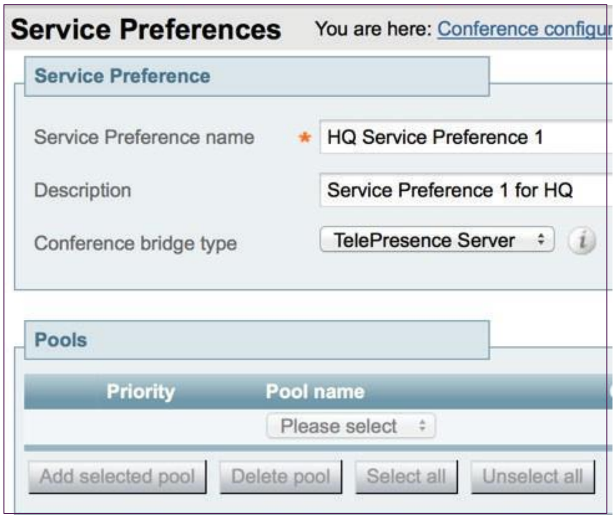
Procedure 6 Create Service preferences

Step 1. Go to **Conference configuration > Service Preferences**.

Step 2. Click **New**.

Step 3. Enter the following values into the relevant fields:

- Service Preference name—**HQ Service Preference 1**
- Conference bridge type—**TelePresence Server**



Service Preferences

You are here: Conference configur

Service Preference

Service Preference name * HQ Service Preference 1

Description: Service Preference 1 for HQ

Conference bridge type: TelePresence Server

Step 4. Click **Add Service Preference**.

Procedure 7 Set up conference bridge pools

To set up a conference bridge pool, you need to create a conference bridge pool and then add the TelePresence Server to it.

Step 1. Navigate to **Conference configuration > Conference bridge** pools and click **New**.

Step 2. Enter the following values into the relevant fields, leaving the other fields at their default values:

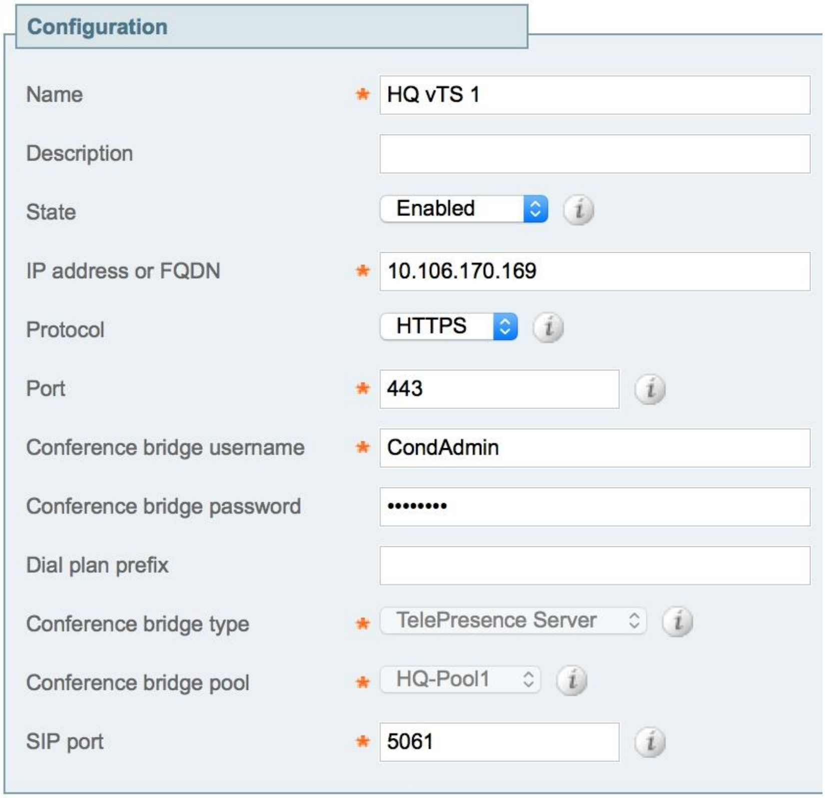
- Pool name—**HQ-Pool1**
- Conference bridge type—**TelePresence Server**

Step 3. Click **Create pool**.

Step 4. On the Conference bridge pools page, click **Create Conference Bridge**.

Step 5. Enter the following values into the relevant fields, leaving the other fields at their default values:

- Name—**HQ vTS 1**
- State—**Enabled**
- IP address of FQDN—**10.106.170.169**
- Protocol – **HTTPS**
- Port—**443**
- Conference bridge username—**CondAdmin**
- Conference bridge password—**[password for the CondAdmin]**
- SIP port—**5061**

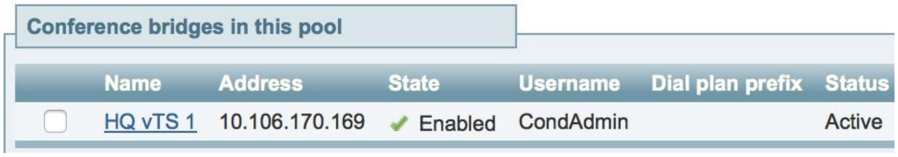


Configuration

Name	*	HQ vTS 1
Description		
State		Enabled
IP address or FQDN	*	10.106.170.169
Protocol		HTTPS
Port	*	443
Conference bridge username	*	CondAdmin
Conference bridge password		••••••••
Dial plan prefix		
Conference bridge type	*	TelePresence Server
Conference bridge pool	*	HQ-Pool1
SIP port	*	5061

Step 6. Click **Create Conference Bridge**.

Step 7. Ensure that under the **Conference bridges in this pool** section, in the Status column, the conference bridge is listed as **Active**.



Conference bridges in this pool

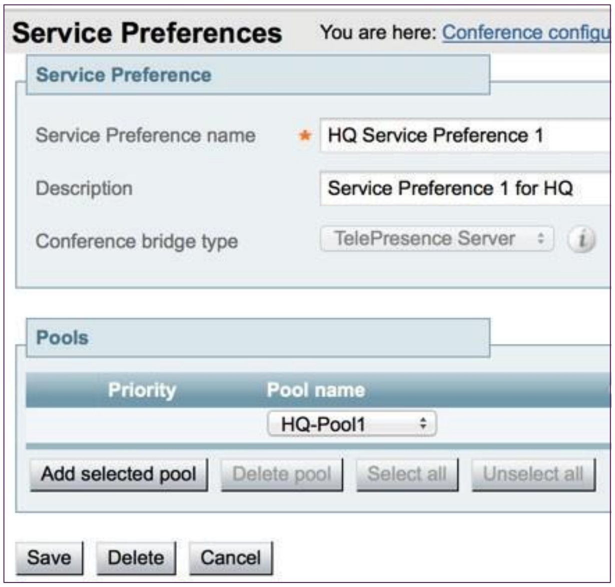
	Name	Address	State	Username	Dial plan prefix	Status
□	HQ vTS 1	10.106.170.169	✓ Enabled	CondAdmin		Active

Procedure 8 Add Conference Bridge Pool in Service preference

Step 1. Go to **Conference configuration > Service Preferences**.

Step 2. Click **HQ Service Preference 1**.

Step 3. Select **HQ-Pool1** under the Pools section.



Service Preferences

You are here: Conference configu

Service Preference

Service Preference name * HQ Service Preference 1

Description Service Preference 1 for HQ

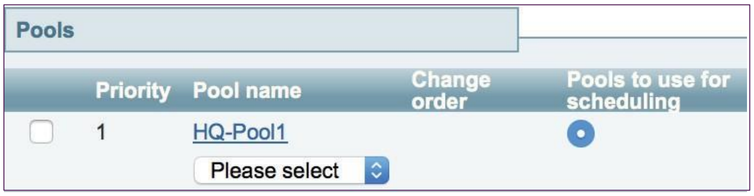
Conference bridge type TelePresence Server

Pools

Priority	Pool name
	HQ-Pool1

Step 4. Click **Add selected pool**.

Step 5. Check the radio button stating **Pools to use for scheduling**.



Pools

	Priority	Pool name	Change order	Pools to use for scheduling
□	1	HQ-Pool1		●
		Please select		

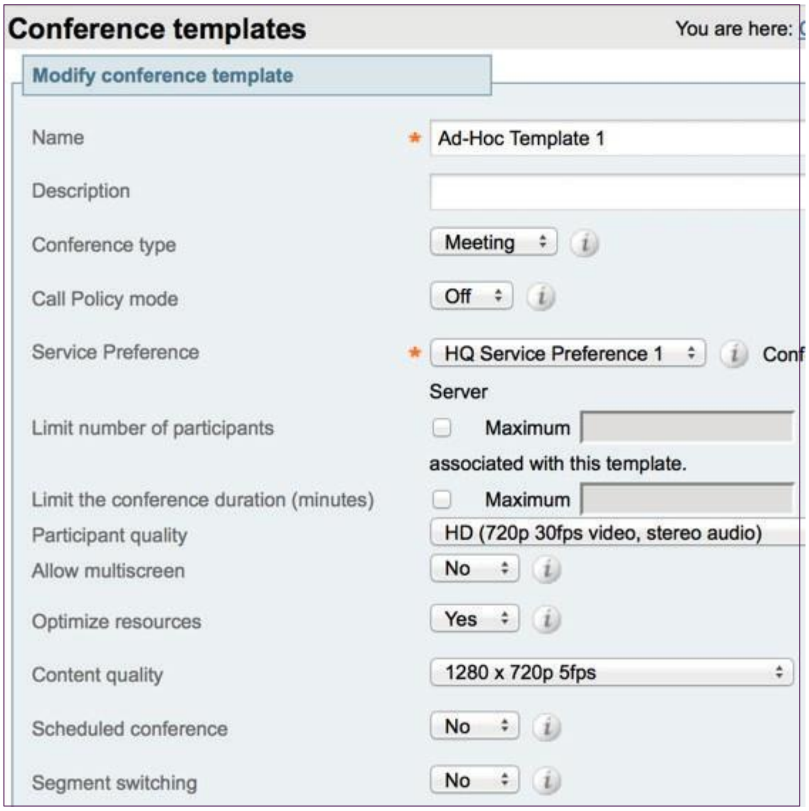
Step 6. Click **Save**.

Procedure 9 Create a conference template for an instant CMR conference

Step 1. Navigate to **Conference configuration > Conference** templates and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name—**Ad-Hoc Template 1**
- Conference type—**Meeting**
- Service preference—**HQ Service Preference 1**
- Participant quality—**HD**
- Optimize resources—**Yes**
- Content quality—**1280 x 720p 5fps**



Conference templates You are here:

Modify conference template

Name *	Ad-Hoc Template 1
Description	
Conference type	Meeting
Call Policy mode	Off
Service Preference *	HQ Service Preference 1 Conf Server
Limit number of participants	□ Maximum associated with this template.
Limit the conference duration (minutes)	□ Maximum
Participant quality	HD (720p 30fps video, stereo audio)
Allow multiscreen	No
Optimize resources	Yes
Content quality	1280 x 720p 5fps
Scheduled conference	No
Segment switching	No

Step 3. Configure other entries as required.

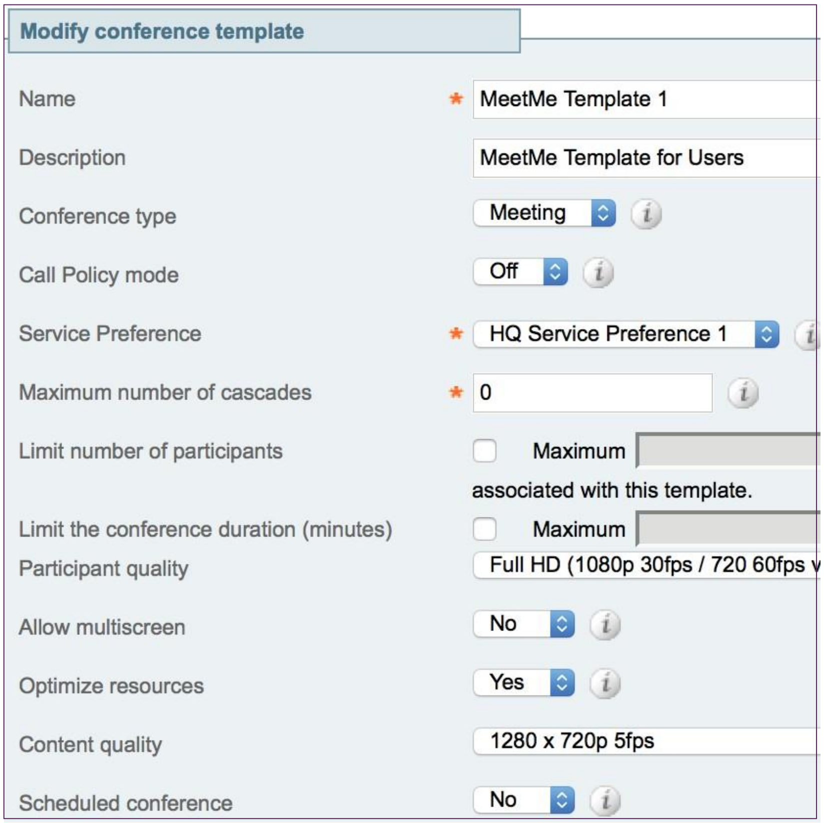
Step 4. Click **Create conference template**.

Procedure 10 Create a conference template for personal CMR conferences

Step 1. Navigate to **Conference configuration** > **Conference** templates and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name—**MeetMe Template 1**
- Conference type—**Meeting**
- Service preference—**HQ Service Preference 1**
- Participant quality—**Full HD**
- Optimize resources—**Yes**
- Content quality—**1280 x 720p 5fps**



Modify conference template

Name *	MeetMe Template 1
Description	MeetMe Template for Users
Conference type	Meeting
Call Policy mode	Off
Service Preference *	HQ Service Preference 1
Maximum number of cascades *	0
Limit number of participants	□ Maximum associated with this template.
Limit the conference duration (minutes)	□ Maximum
Participant quality	Full HD (1080p 30fps / 720 60fps v
Allow multiscreen	No
Optimize resources	Yes
Content quality	1280 x 720p 5fps
Scheduled conference	No

Step 3. Configure other entries as required.

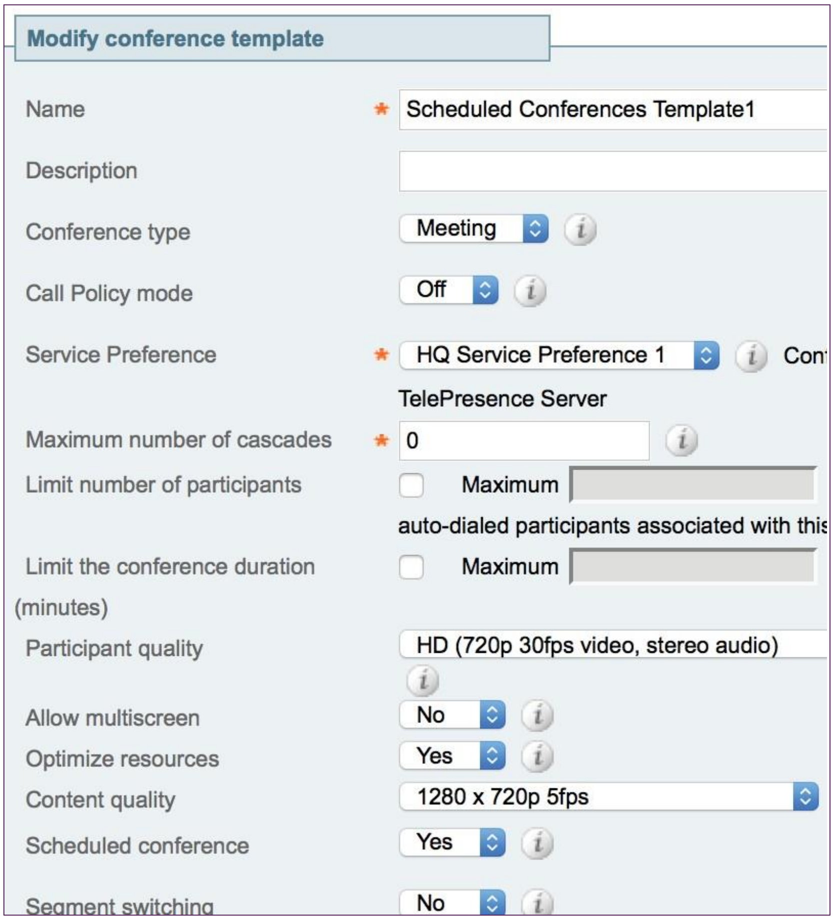
Step 4. Click **Create conference template**.

Procedure 11 Create a conference template for scheduled CMR conference

Step 1. Navigate to **Conference configuration > Conference** templates and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name—**Scheduled Conferences Template 1**
- Conference type—**Meeting**
- Service preference—**HQ Service Preference 1**
- Participant quality—**HD**
- Optimize resources—**Yes**
- Content quality—**1280 x 720p 5fps**
- Scheduled Conference—**Yes**



Modify conference template

Name *	Scheduled Conferences Template1
Description	
Conference type	Meeting
Call Policy mode	Off
Service Preference *	HQ Service Preference 1 Con TelePresence Server
Maximum number of cascades *	0
Limit number of participants	□ Maximum auto-dialed participants associated with this
Limit the conference duration (minutes)	□ Maximum
Participant quality	HD (720p 30fps video, stereo audio)
Allow multiscreen	No
Optimize resources	Yes
Content quality	1280 x 720p 5fps
Scheduled conference	Yes
Segment switching	No

Step 3. Configure other entries as required.

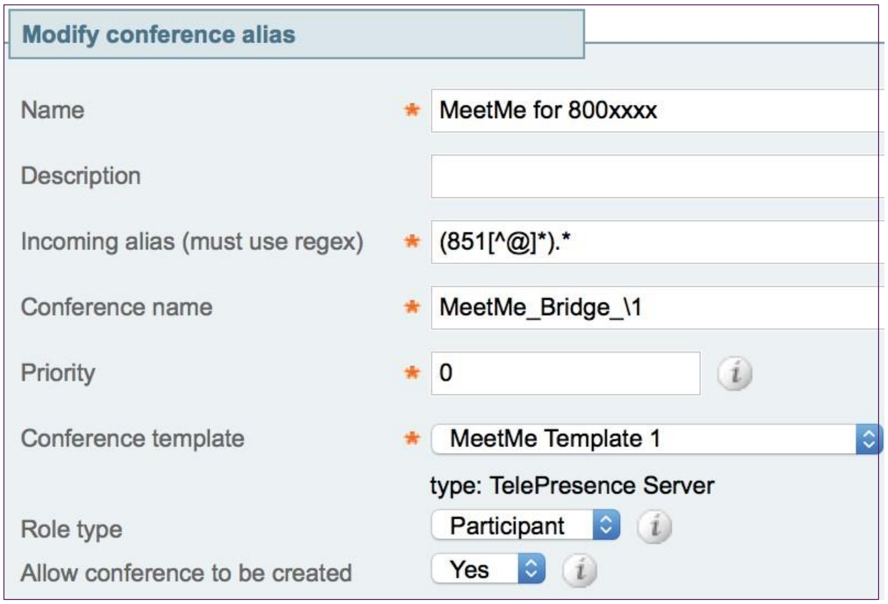
Step 4. Click **Create conference template**.

Procedure 12 Create a conference alias for an personal CMR conferences

Step 1. Navigate to **Conference configuration > Conference aliases** and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name—**MeetMe for 800xxxx**
- Incoming Alias (must use regex)—**(851[^@]*).***
- Conference name—**MeetMe_Bridge_\1**
- Priority—**0**
- Conference template—**MeetMe Template 1**
- Role type—**Participant**
- Allow conference to be created—**Yes**



Modify conference alias

Name *	MeetMe for 800xxxx
Description	
Incoming alias (must use regex) *	(851[^@]*).*
Conference name *	MeetMe_Bridge_\1
Priority *	0
Conference template *	MeetMe Template 1 type: TelePresence Server
Role type	Participant
Allow conference to be created	Yes

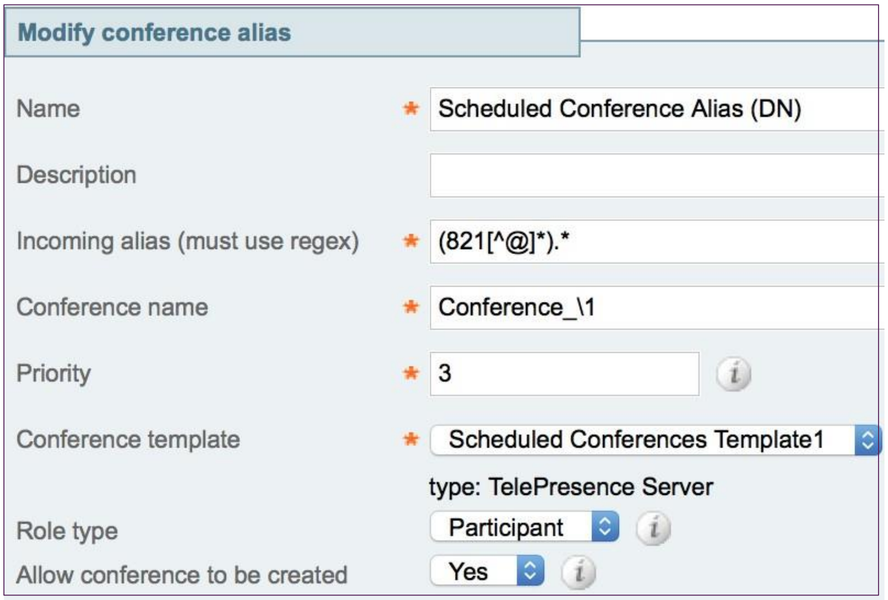
Step 3. Click **Create conference alias**.

Procedure 13 Create a conference alias for an scheduled CMR conference

Step 1. Navigate to **Conference configuration > Conference aliases** and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name—**Scheduled Conference Alias (DN)**
- Incoming Alias (must use regex)—**(821[^@]*).***
- Conference name—**Conference_\1**
- Priority—**3**
- Conference template—**Scheduled Conferences Template1**
- Role type—**Participant**
- Allow conference to be created—**Yes**



Modify conference alias

Name *	Scheduled Conference Alias (DN)
Description	
Incoming alias (must use regex) *	(821[^@]*).*
Conference name *	Conference_\1
Priority *	3
Conference template *	Scheduled Conferences Template1 type: TelePresence Server
Role type	Participant
Allow conference to be created	Yes

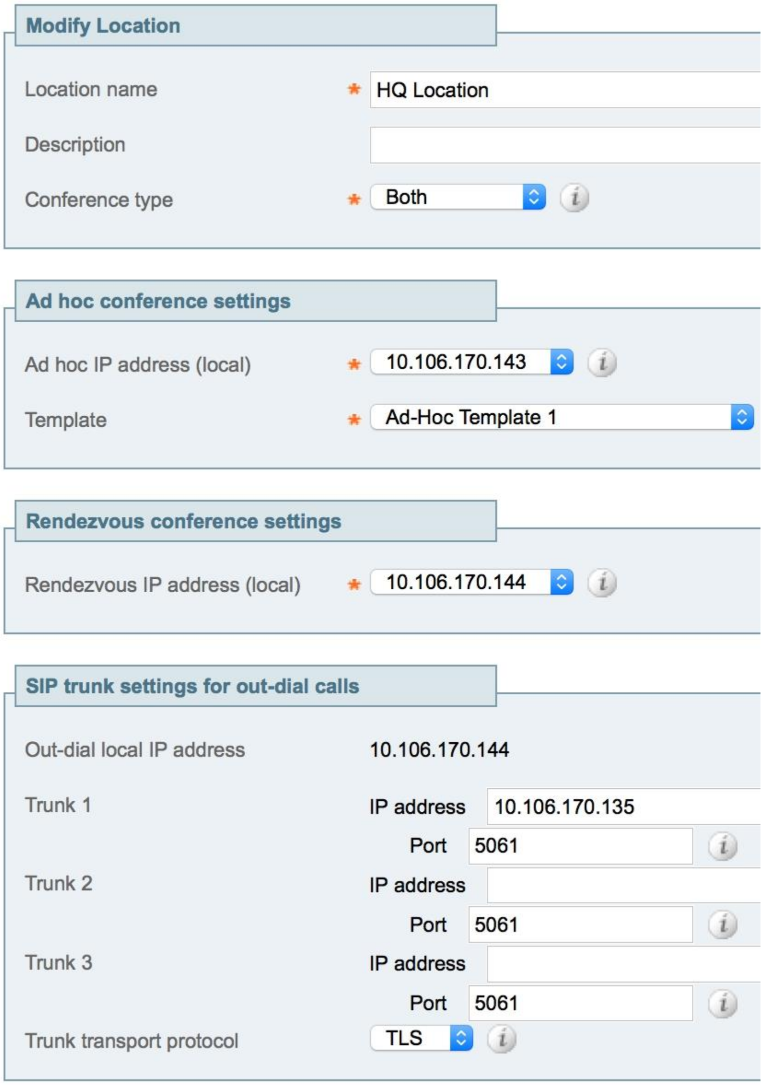
Step 3. Click **Create conference alias**.

Procedure 14 Create locations in Conductor

Step 1. Navigate to **Conference configuration > Locations** and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Location name—**HQ Location**
- Conference type—**Both**
- Ad hoc IP address (local)— **10.106.170.143**
- Template—**Ad-Hoc Template 1**
- Rendezvous IP address (local)—**10.106.170.144**
- Trunk IP address—**10.106.170.135**
- Trunk port—**5061**
- Trunk transport protocol—**TLS**



Modify Location

Location name *	HQ Location
Description	
Conference type *	Both

Ad hoc conference settings

Ad hoc IP address (local) *	10.106.170.143
Template *	Ad-Hoc Template 1

Rendezvous conference settings

Rendezvous IP address (local) *	10.106.170.144

SIP trunk settings for out-dial calls

Out-dial local IP address	10.106.170.144	
Trunk 1	IP address	10.106.170.135
	Port	5061
Trunk 2	IP address	
	Port	5061
Trunk 3	IP address	
	Port	5061
Trunk transport protocol	TLS	

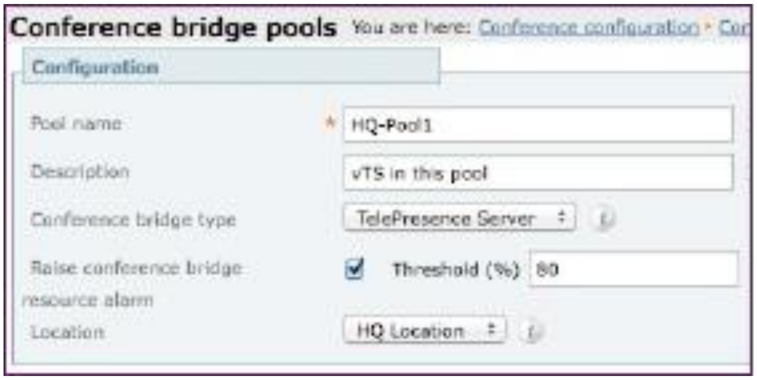
Step 3. Click Add location.

Procedure 15 Add locations to conference bridge pools

Step 1. Log into TelePresence Conductor as a user with administrator rights.

Step 2. Navigate to **Conference configuration > Conference bridge pools**, and click **HQ-Pool1**.

Step 3. Select the Location as **HQ Location**.



Conference bridge pools You are here: Conference configuration › Con

Configuration

Pool name * HQ-Pool1

Description vTS in this pool

Conference bridge type TelePresence Server

Raise conference bridge resource alarm ☑ Threshold (%) 80

Location HQ Location

Step 4. Click on **Save**.

Tech Tip

For TelePresence Conductor redundancy, please refer the latest Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide.

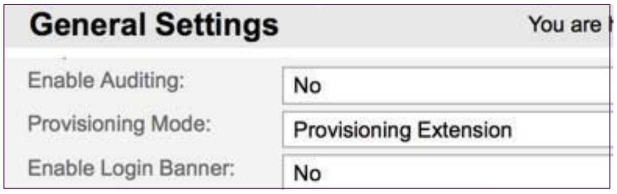
Configuring Cisco TelePresence Management Suite (TMS)

PROCESS

Procedure 1 Enable TMSPE on TMS

Step 1. Log into TMS as a user with administrator rights.

Step 2. Navigate to **Administrative Tools > Configuration > General Settings** and set the **Provisioning Mode** field as **Provisioning Extension**.



General Settings

You are

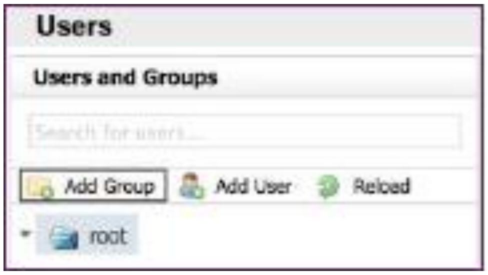
Enable Auditing:	No
Provisioning Mode:	Provisioning Extension
Enable Login Banner:	No

Step 3. Click on **Save**.

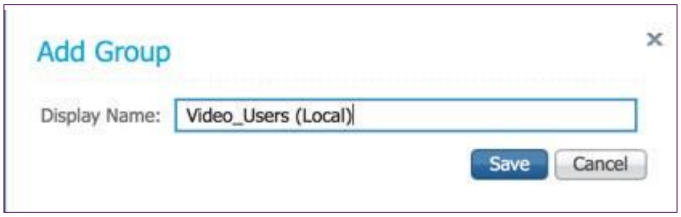
Procedure 2 Setup users on TMS

Step 1. Navigate to Systems > Provisioning > Users.

Step 2. Click on Root and then click on Add Group.

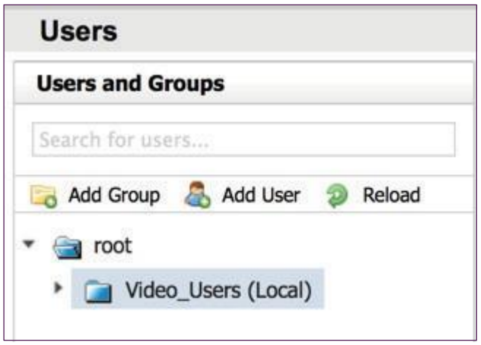


Step 3. Enter **Video_Users (Local)** as Display Name when the Add Group dialog comes up and click Save.


Add Group

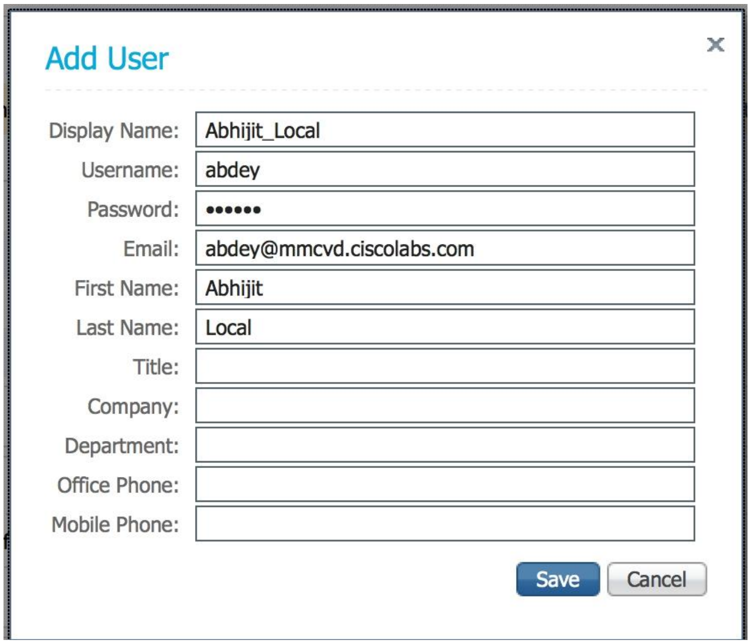
Display Name: Video_Users (Local)

Step 4. Click on Add User.



Step 5. Enter the following into the relevant fields, leaving other fields at their default values:

- Display Name—**Abhijit_Local**
- Username—**abdey**
- Password—**[Password]**
- Email—**abdey@mmcvd.ciscolabs.com**
- Last Name—**Local**



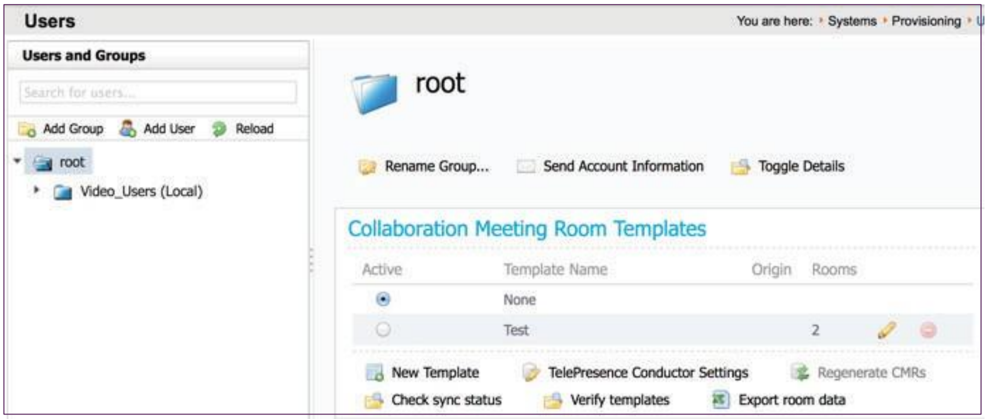
Add User

Display Name:	Abhijit_Local
Username:	abdey
Password:	••••••
Email:	abdey@mmcvd.ciscolabs.com
First Name:	Abhijit
Last Name:	Local
Title:	
Company:	
Department:	
Office Phone:	
Mobile Phone:	

Step 6. Click Save.

Procedure 3 Add Conductor for CMR on TMS

Step 1. Navigate to **Systems** > **Provisioning** > **Users**.



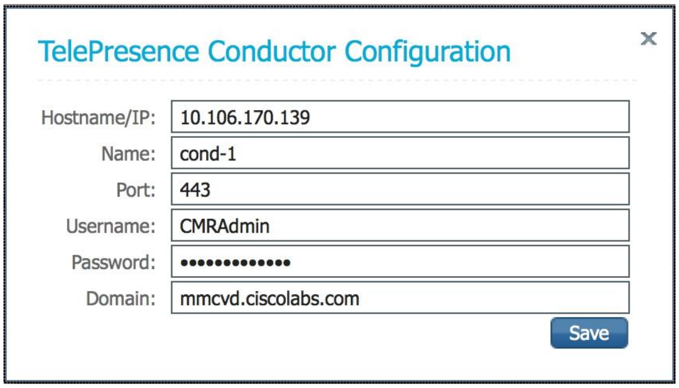
Collaboration Meeting Room Templates

Active	Template Name	Origin	Rooms
●	None		
○	Test		2

Step 2. Under **Collaboration Meeting Room Templates**, click **TelePresence Conductor Settings**.

Step 3. Click **Add New** and enter the following into the relevant fields, leaving other fields at their default values:

- Hostname/IP—**10.106.170.139**
- Name—**cond-1**
- Port—**443**
- Username—**CMRAdmin**
- Password—**[Password]**
- Domain—**mmcvd.ciscolabs.com**



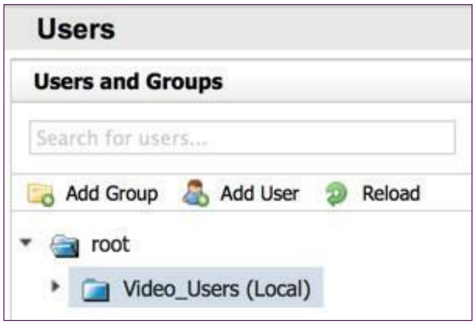
TelePresence Conductor Configuration

Hostname/IP:	10.106.170.139
Name:	cond-1
Port:	443
Username:	CMRAdmin
Password:	•••••••••••••
Domain:	mmcvd.ciscolabs.com

Step 4. Click **Save**.

Procedure 4 Setup CMRs on TMS

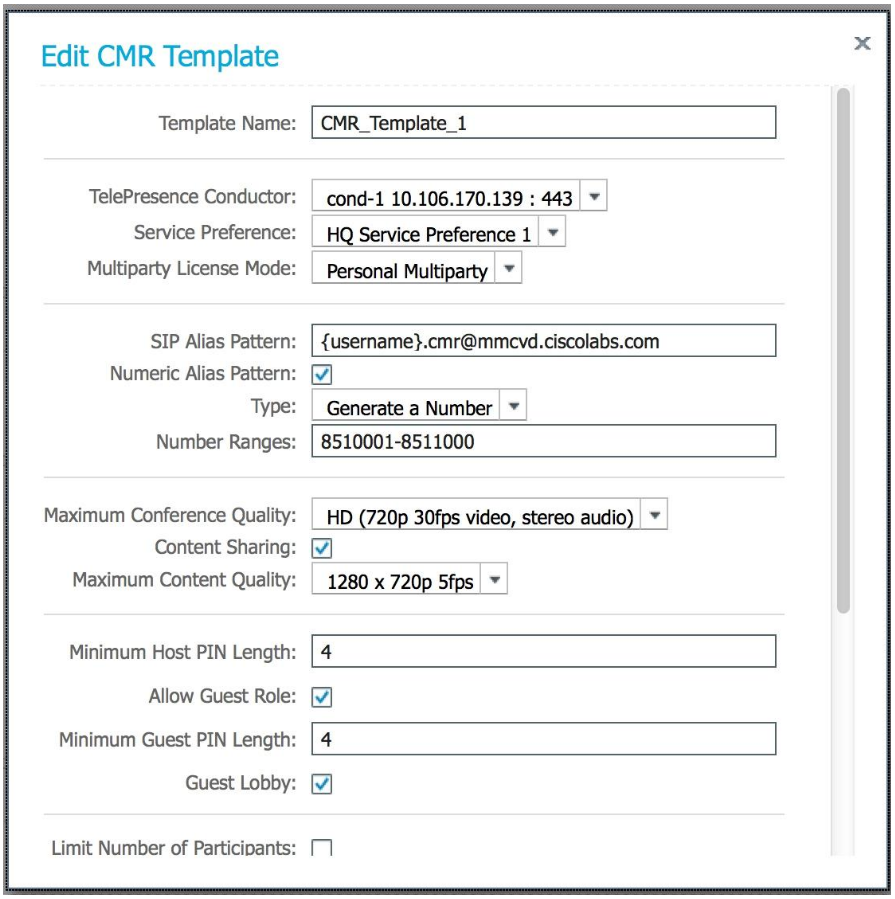
Step 1. Navigate to Systems > Provisioning > Users and click on Video_Users (Local).



Step 2. Under Collaboration Meeting Room Templates, click New Template.

Step 3. Enter the following into the relevant fields, leaving the other fields at their default values:

- Template Name–**CMR_Template_1**
- TelePresence Conductor–**cond-1 10.106.170.139 : 443**
- Service Preference–**HQ Service Preference 1**
- Multiparty License Mode – **Personal Multiparty**
- SIP Alias Pattern– **{username}.cmr@mmcvd.ciscolabs.com**
- Numeric Alias Pattern–**Selected**
- Type–**Generate a Number**
- Number Ranges–**8510001-8511000**
- Maximum Conference Quality–**HD (720p 30 fps video, stereo audio)**
- Content Sharing–**Selected**
- Maximum Content Quality–**1280 x 720p 5fps**
- Optimize Resources–**Selected**



Edit CMR Template

Template Name: CMR_Template_1

TelePresence Conductor: cond-1 10.106.170.139 : 443

Service Preference: HQ Service Preference 1

Multiparty License Mode: Personal Multiparty

SIP Alias Pattern: {username}.cmr@mmcvd.ciscolabs.com

Numeric Alias Pattern: ☑

Type: Generate a Number

Number Ranges: 8510001-8511000

Maximum Conference Quality: HD (720p 30fps video, stereo audio)

Content Sharing: ☑

Maximum Content Quality: 1280 x 720p 5fps

Minimum Host PIN Length: 4

Allow Guest Role: ☑

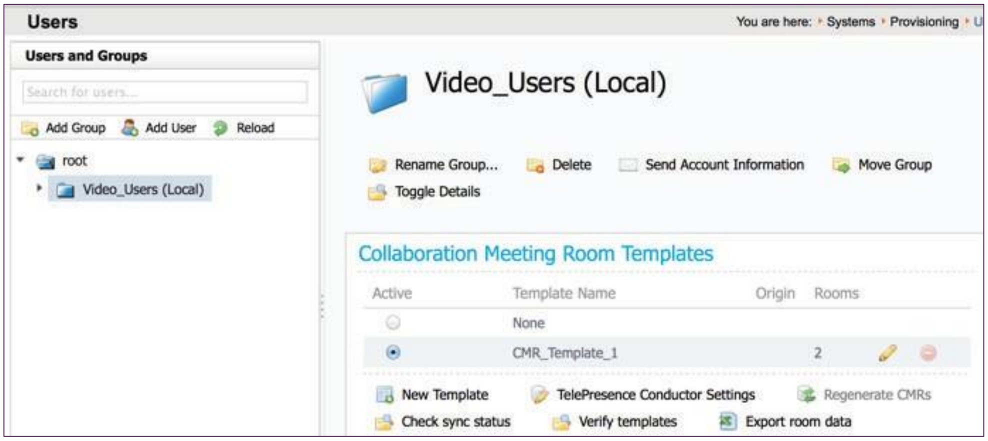
Minimum Guest PIN Length: 4

Guest Lobby: ☑

Limit Number of Participants: □

Step 4. Click **Save**.

Step 5. Select the radio button for **CMR_Template_1** under the **Collaboration Meeting Room** Templates and click **Yes**.



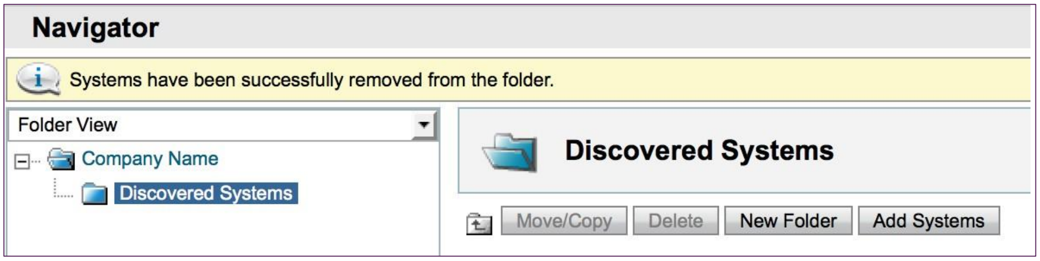
Active	Template Name	Origin	Rooms
○	None		
●	CMR_Template_1		2

The CMR template is applied to all the users in **Video_Users (Local)** group.

Procedure 5 Add Conductor for scheduling on TMS

Step 1. Navigate to **Systems > Navigator**.

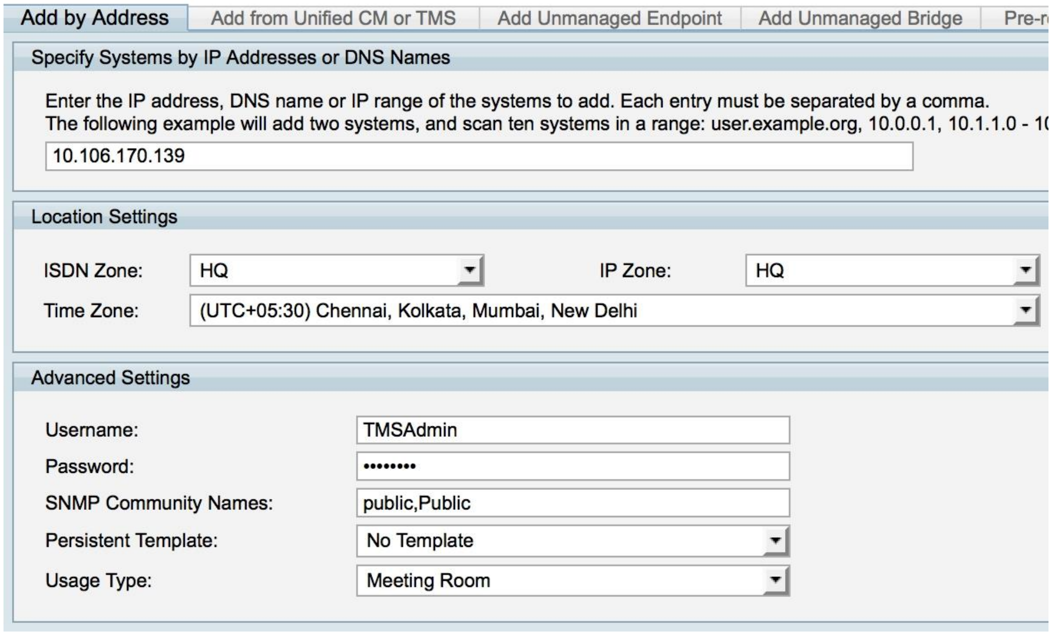
Step 2. Click on **Discovered Systems** on the left folder view and then click on **Add Systems** on the right Discovered Systems section.



Systems have been successfully removed from the folder.

Step 3. Enter the following into the relevant fields:

- Specify Systems by IP Addresses or DNS Names—**10.106.170.139**
- ISDN Zones—**HQ**
- IP Zones—**HQ**
- Time Zones—**(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi**
- Usernames—**TMSAdmin**
- Passwords—**[Password]**
- Persistent Template—**No Template**
- Usage Type—**Other**



Specify Systems by IP Addresses or DNS Names

Enter the IP address, DNS name or IP range of the systems to add. Each entry must be separated by a comma.
The following example will add two systems, and scan ten systems in a range: user.example.org, 10.0.0.1, 10.1.1.0 - 1(

10.106.170.139

Location Settings

ISDN Zone: HQ   IP Zone: HQ

Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Advanced Settings

Username: TMSAdmin

Password: ••••••••

SNMP Community Names: public,Public

Persistent Template: No Template

Usage Type: Meeting Room

Step 4. Click **Next**.

Step 5. Click **Finish Adding Systems**.

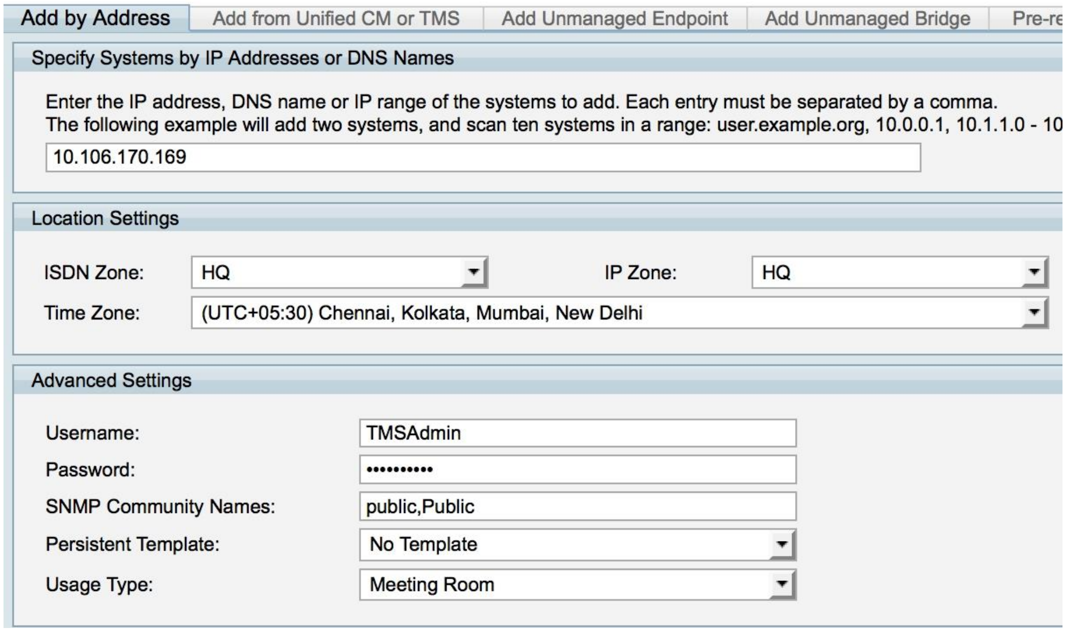
Procedure 6 Add TelePresence Server for scheduling on TMS

Step 1. Navigate to **Systems > Navigator**.

Step 2. Click on **Discovered Systems** on the left folder view and then click on **Add Systems** on the right Discovered Systems section.

Step 3. Enter the following into the relevant fields:

- Specify Systems by IP Addresses or DNS Names—**10.106.170.169**
- ISDN Zone—**HQ**
- IP Zone— **HQ**
- Time Zone—**(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi**
- Username—**TMSAdmin**
- Password—**[Password]**
- Persistent Template—**No Template**
- Usage Type—**Other**



Specify Systems by IP Addresses or DNS Names

Enter the IP address, DNS name or IP range of the systems to add. Each entry must be separated by a comma.
The following example will add two systems, and scan ten systems in a range: user.example.org, 10.0.0.1, 10.1.1.0 - 10

10.106.170.169

Location Settings

ISDN Zone: HQ
IP Zone: HQ
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Advanced Settings

Username: TMSAdmin
Password: ••••••••••
SNMP Community Names: public,Public
Persistent Template: No Template
Usage Type: Meeting Room

Step 4. Click **Next**.

Step 5. Click **Finish Adding Systems**.

Procedure 7 Create conference alias on TMS

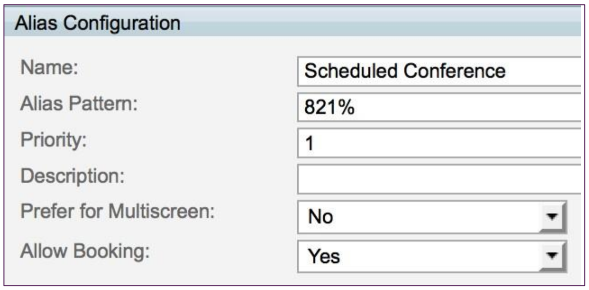
Step 1. Navigate to **Systems > Navigator**.

Step 2. Click on **cond-1** under Discovered Systems and then click **on TelePresence Conductor** tab.

Step 3. Click **New**.

Step 4. Enter the following into the relevant fields:

- Name—**Scheduled Conference**
- Alias Pattern—**821%**
- Priority—**1**
- Prefer for Multiscreen—**No**
- Allow Booking—**Yes**



Alias Configuration

Name:	Scheduled Conference
Alias Pattern:	821%
Priority:	1
Description:	
Prefer for Multiscreen:	No
Allow Booking:	Yes

Step 5. Click **Save**.

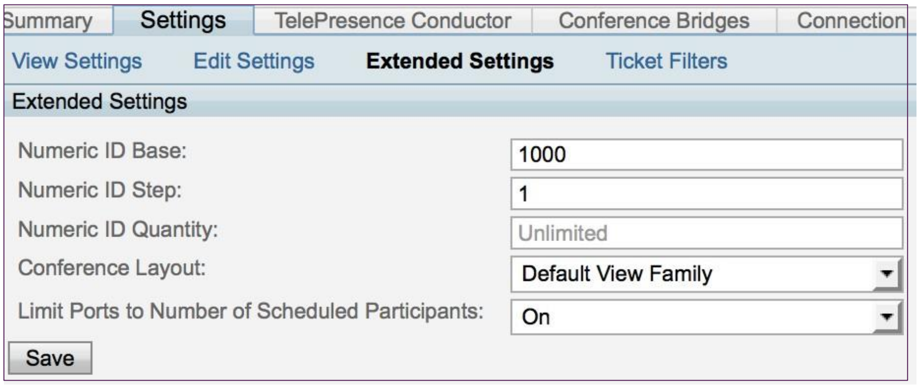
Procedure 8 Configure conference settings on TMS

Step 1. Navigate to **Systems > Navigator**.

Step 2. Click on **cond-1** under Discovered Systems and then click **on Settings > Extended Settings** tab.

Step 3. Enter the following into the relevant fields:

- Numeric ID Base—**1000**
- Numeric ID Step—**1**



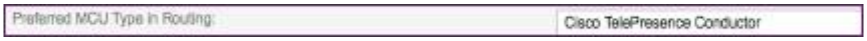
Extended Settings

Numeric ID Base:	1000
Numeric ID Step:	1
Numeric ID Quantity:	Unlimited
Conference Layout:	Default View Family
Limit Ports to Number of Scheduled Participants:	On

Step 4. Click **Save**.

Step 5. Navigate to **Administrative Tools > Configuration > Conference Settings**.

Step 6. Enter **Preferred MCU type in routing as Cisco TelePresence Conductor**.



Preferred MCU Type in Routing:	Cisco TelePresence Conductor

Step 7. Click **Save**.

Configuring Cisco Unified Communications Manager (Unified CM)

Easy Access Configuration Sheet

Cisco UCM Configuration Requirements		
Item	CVD Configuration	Site Specific Configuration
Video bandwidth for video region	32256	
Route pattern for personal and scheduled CMR conferences	8[2-5]XXXXX	
Route pattern for TCS recording alias	861XXXX	
URI pattern for personal CMR conferences	user.cmr@mmcvd.ciscolabs.com	

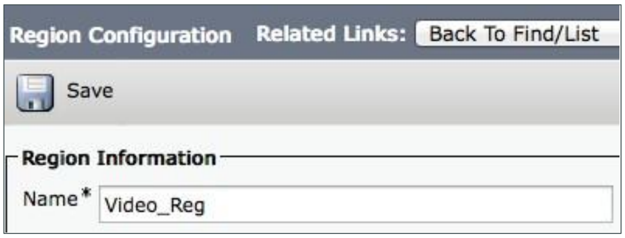
PROCESS

1. Configure region for video
2. Configure device pool for video and add the video region
3. Configure Unified CM trunk to TelePresence Conductor for personal and scheduled CMR conferences
4. Configure Unified CM trunk to Conductor for instant CMR conferences
5. Configure SIP Trunk Security Profile for TCS (recording only)
6. Configure SIP Profile for TCS (recording only)
7. Configure Unified CM directory number route pattern for personal and scheduled CMR conferences
8. Configure Unified CM directory number route pattern for TCS (recording only)
9. Configure Unified CM SIP route pattern for personal CMR conferences
10. Configure Conductor as conference bridge
11. Configure MRG and MRGL for video and add Conductor to this MRG
12. Add this MRGL to the device profile for video

Procedure 1 Configure region for video

Step 1. Navigate to **System > Region Information > Region**, and click **Add New** in order to create a new Region.

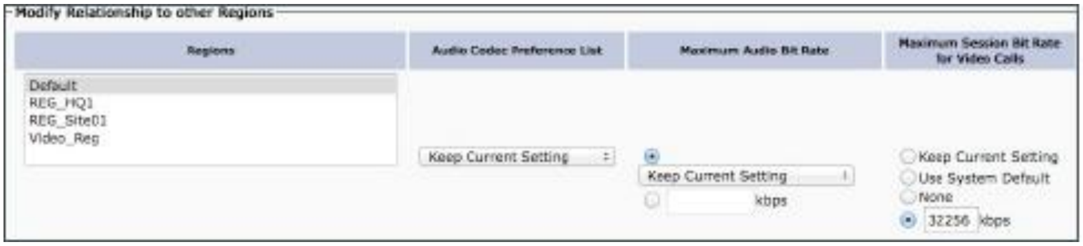
Step 2. In **Name**, enter **Video_Reg**, and then click **Save**.



Name* Video_Reg

Step 3. Under **Regions**, select **Default**.

Step 4. Under **Maximum Session Bit Rate for Video Calls**, enter **32256** kbps.



Regions: Default (selected), REG_HQ1, REG_Site01, Video_Reg

Audio Codec Preference List: Keep Current Setting

Maximum Audio Bit Rate: ● Keep Current Setting; ○ kbps

Maximum Session Bit Rate for Video Calls: ○ Keep Current Setting; ○ Use System Default; ○ None; ● 32256 kbps

This CVD is using 32256 as the configured video bandwidth for this region.

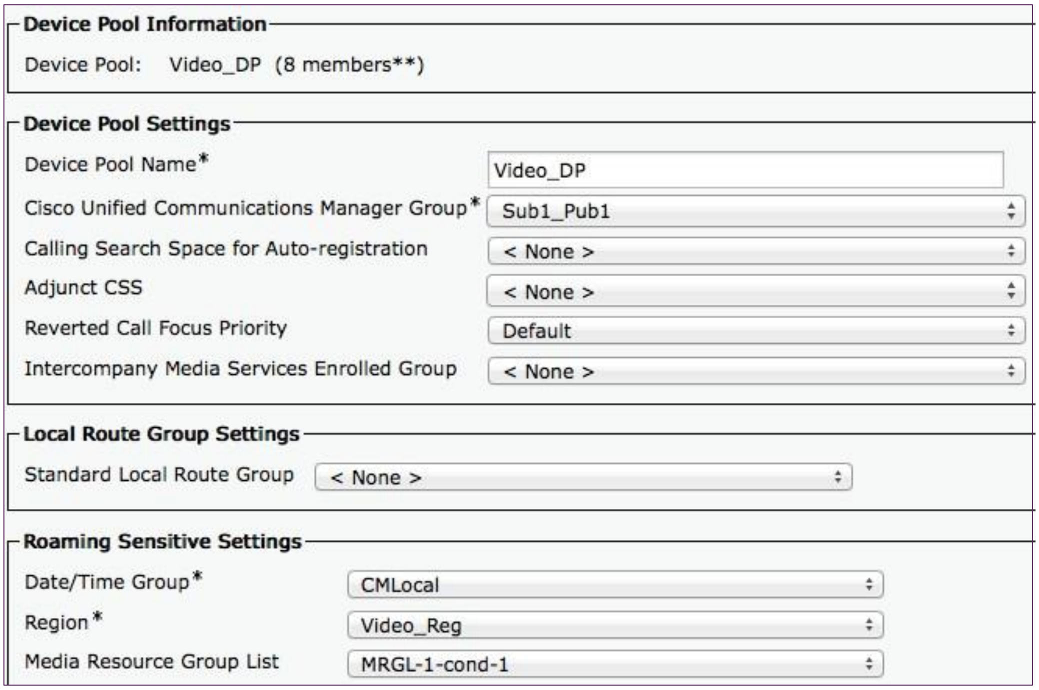
Step 5. Click **Save**.

Procedure 2 Configure device pool for video and add the video region

Step 1. Navigate to **System > Device Pool**, and then click **Add New** in order to add a new device pool.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Device Pool Name—**Video_DP**
- Cisco Unified Communications Manager Group - **Sub1_Pub1**
- Date/Time Group - **CMLocal**
- Region—**Video_Reg**



Device Pool Information

Device Pool: Video_DP (8 members**)

Device Pool Settings

Device Pool Name*	Video_DP
Cisco Unified Communications Manager Group*	Sub1_Pub1
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >

Local Route Group Settings

Standard Local Route Group	< None >

Roaming Sensitive Settings

Date/Time Group*	CMLocal
Region*	Video_Reg
Media Resource Group List	MRGL-1-cond-1

Step 3. Click **Save**.

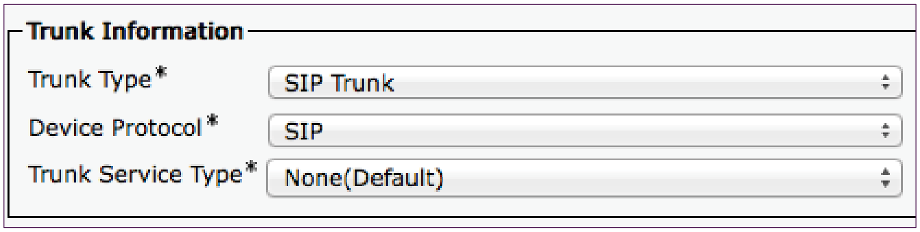
Procedure 3 Configure Unified CM trunk to TelePresence Conductor for personal and scheduled CMR conferences

A *trunk* is a communications channel on Unified CM that enables it to connect to other servers. Using one or more trunks, Unified CM can receive or place voice, video, and encrypted calls, exchange real-time event information, and communicate in other ways with call control servers and other external servers.

Step 1. Navigate to **Device > Trunk**, and then click **Add New** in order to create a new SIP trunk.

Step 2. Enter the following into the relevant fields:

- Trunk Type—**SIP Trunk**
- Device Protocol—**SIP**
- Trunk Service Type—**None(Default)**



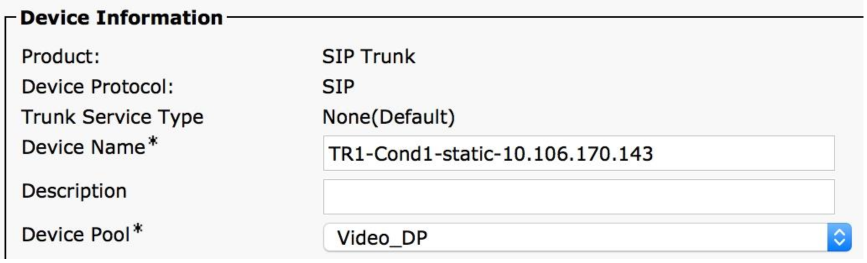
Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Step 3. Click **Next**.

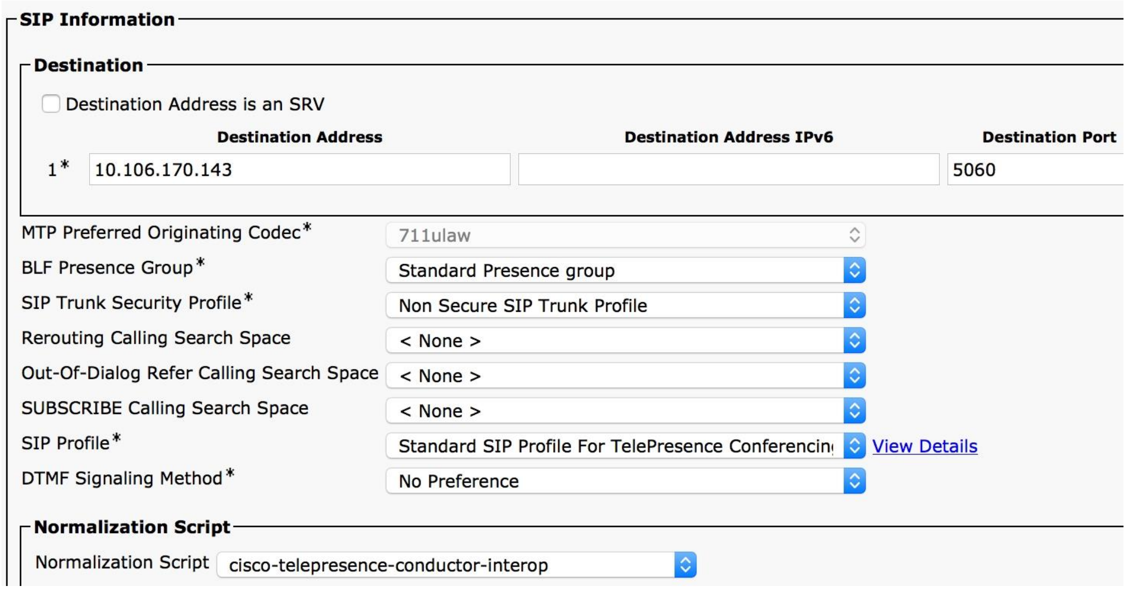
Step 4. Enter the following into the relevant fields, leaving other fields at their default values:

- Device Name—**TR1-Cond1-static-10.106.170.143**
- Device Pool—**Video_DP**
- Destination Address—**10.106.170.143**
- Destination Port—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile**
- SIP Profile—**Standard SIP Profile for TelePresence Conferencing**
- Normalization Script—**cisco-telepresence-conductor-interop**



Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TR1-Cond1-static-10.106.170.143
Description	
Device Pool*	Video_DP



SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.170.143		5060

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile For TelePresence Conferencin
DTMF Signaling Method*	No Preference

Normalization Script

Normalization Script: cisco-telepresence-conductor-interop

Step 5. Click **Save**.

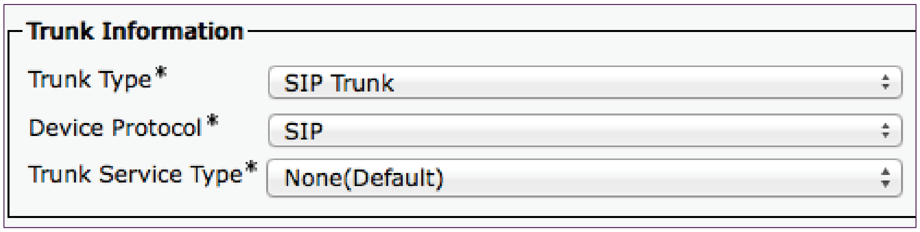
Step 6. Click **Reset**.

Procedure 4 Configure Unified CM trunk to Conductor for instant CMR conferences

Step 1. Navigate to **Device > Trunk**, and then click **Add New** in order to create a new SIP trunk.

Step 2. Enter the following into the relevant fields:

- Trunk Type—**SIP Trunk**
- Device Protocol—**SIP**
- Trunk Service Type—**None(Default)**



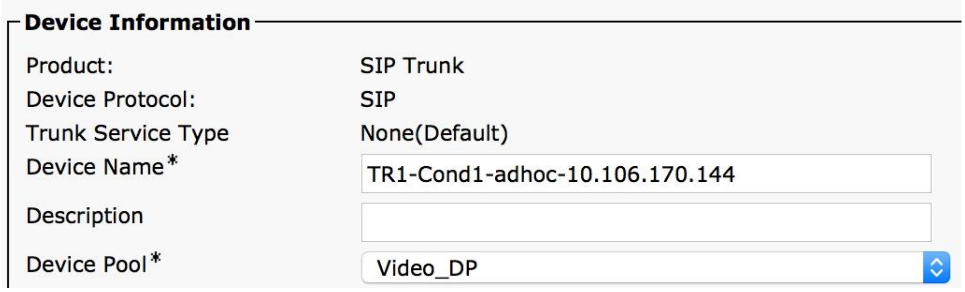
Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Step 3. Click **Next**.

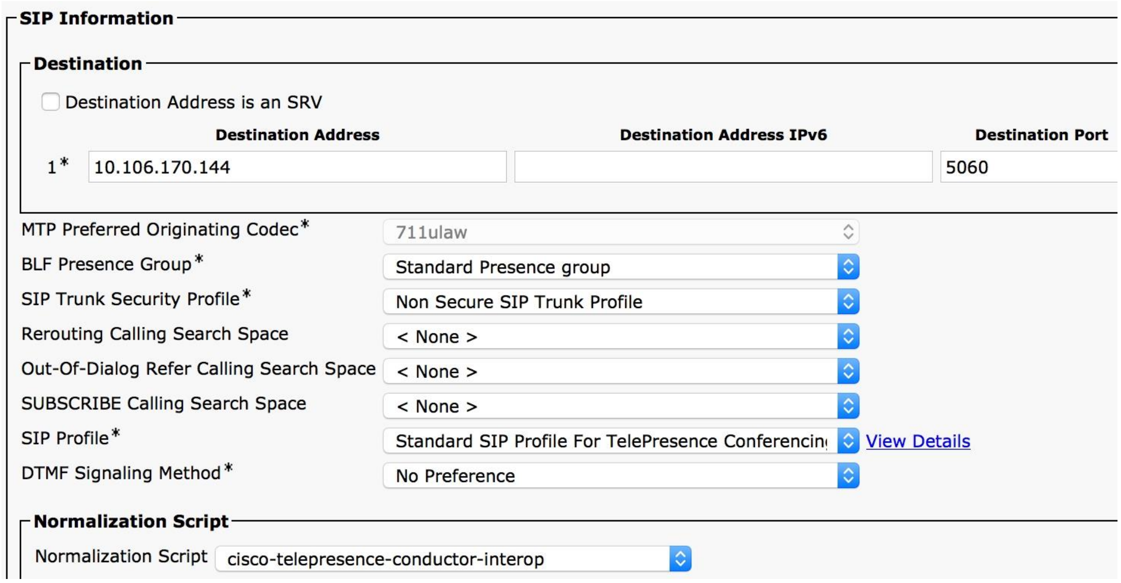
Step 4. Enter the following into the relevant fields, leaving other fields at their default values:

- Device Name—**TR1-Cond1-adhoc-10.106.170.144**
- Device Pool—Video_DP
- Destination Address—**10.106.170.144**
- Destination Port—**5060**
- SIP Trunk Security Profile—Non Secure SIP Trunk Profile
- SIP Profile—Standard SIP Profile for TelePresence Conferencing
- Normalization Script—cisco-telepresence-conductor-interop



Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TR1-Cond1-adhoc-10.106.170.144
Description	
Device Pool*	Video_DP



SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.170.144		5060

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile For TelePresence Conferencin View Details
DTMF Signaling Method*	No Preference

Normalization Script

Normalization Script	cisco-telepresence-conductor-interop

Step 5. Click Save.

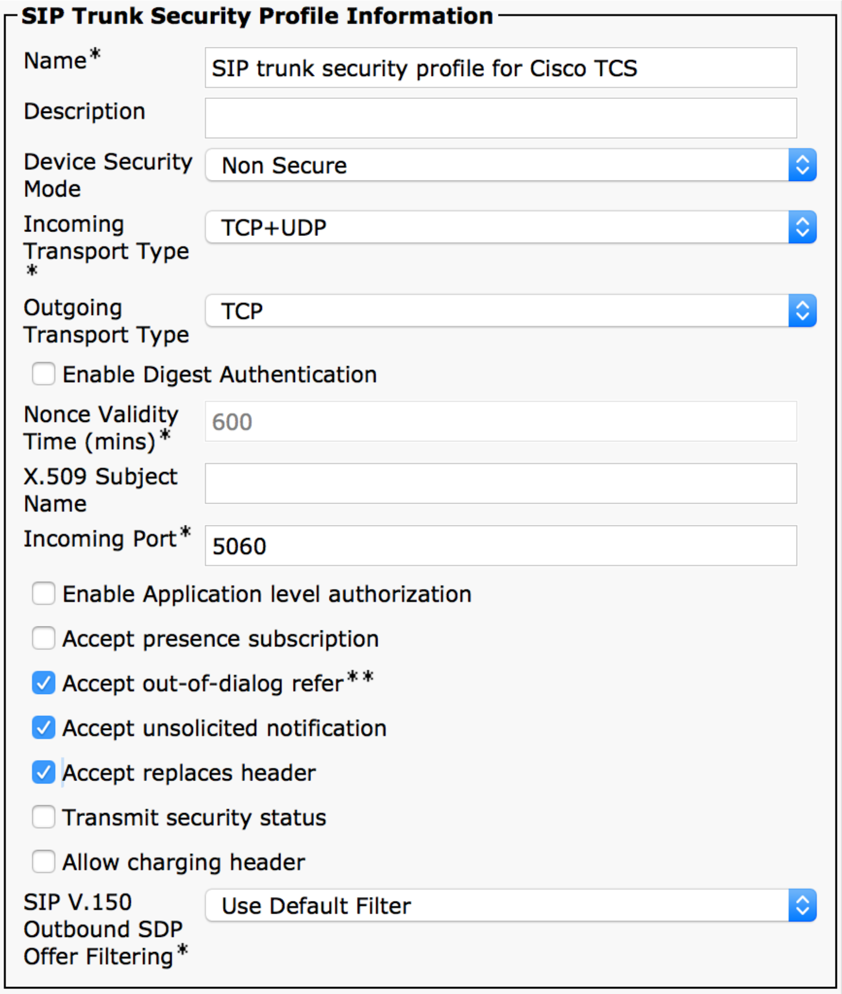
Step 6. Click Reset.

Procedure 5 Configure SIP Trunk Security Profile for TCS (recording only)

Step 1. Navigate to **System** > **Security** > **SIP Trunk Security Profile**, and then click **Add New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name - **SIP trunk security profile for Cisco TCS**
- Accept out-of-dialog refer – **checked**
- Accept unsolicited notification – **checked**
- Accept replaces header – **checked**



SIP Trunk Security Profile Information

Name*	SIP trunk security profile for Cisco TCS
Description	
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP

□ Enable Digest Authentication

Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060

□ Enable Application level authorization

□ Accept presence subscription

☑ Accept out-of-dialog refer**

☑ Accept unsolicited notification

☑ Accept replaces header

□ Transmit security status

□ Allow charging header

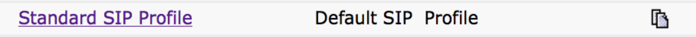
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Step 3. Click **Save**.

Procedure 6 Configure SIP Profile for TCS (recording only)

Step 1. Navigate to **Device > Device Settings > SIP Profile**, and then click **Find.**

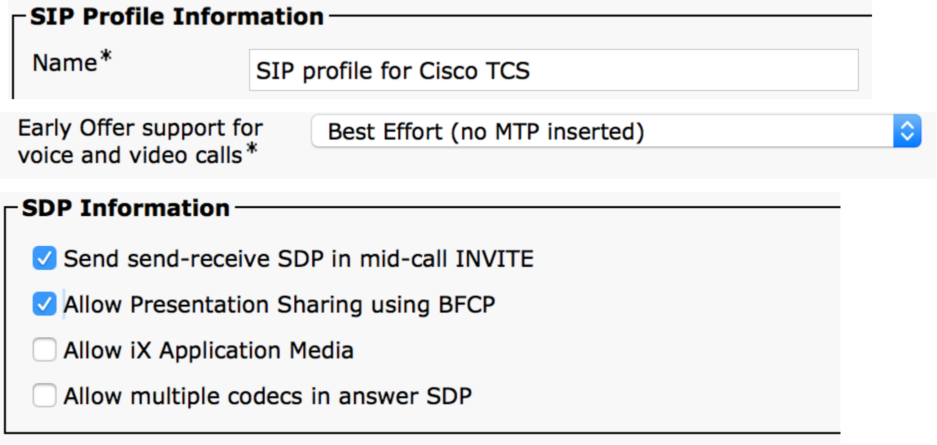
Step 2. Click on the **copy** icon on the right side of **Standard SIP Profile**.



Standard SIP Profile Default SIP Profile

Step 3. Enter the following into the relevant fields, leaving other fields at their default values:

- Name - **SIP profile for Cisco TCS**
- Early Offer support for voice and video calls – **Best Effort (no MTP inserted)**
- Send send-receive SDP in mid-call INVITE – **checked**
- Allow Presentation Sharing using BFCP – **checked**



SIP Profile Information

Name* SIP profile for Cisco TCS

Early Offer support for voice and video calls* Best Effort (no MTP inserted)

SDP Information

☑ Send send-receive SDP in mid-call INVITE

☑ Allow Presentation Sharing using BFCP

□ Allow iX Application Media

□ Allow multiple codecs in answer SDP

Step 4. Click **Save**.

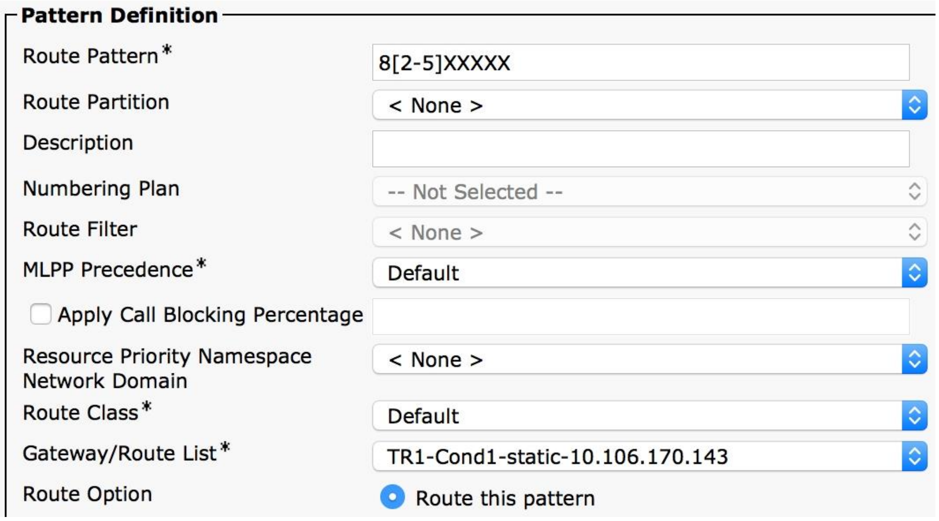
Procedure 7 Configure Unified CM directory number route pattern for personal and scheduled CMR conferences

This procedure describes configuring the Unified CM route pattern to match the SIP trunk to TelePresence Conductor for personal and scheduled CMR conferences.

Step 1. Navigate to **Call Routing > Route/Hunt > Route Pattern**, and then click **Add New** in order to create a new route pattern.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Route Pattern—**8[2-5]XXXXX**
- Gateway/Route List—**TR1-Cond1-static-10.106.170.143**



Pattern Definition

Route Pattern*	8[2-5]XXXXX
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	TR1-Cond1-static-10.106.170.143
Route Option	● Route this pattern

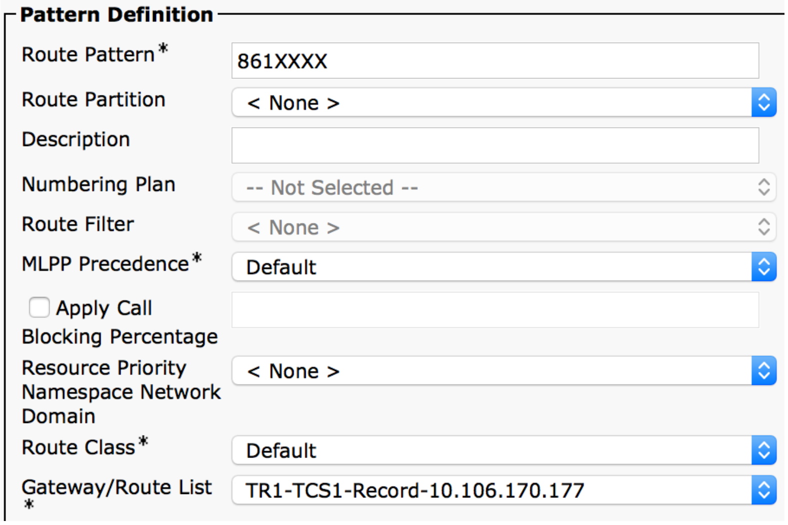
Step 3. Click **Save**.

Procedure 8 Configure Unified CM directory number route pattern for TCS (recording only)

Step 1. Navigate to **Call Routing > Route/Hunt > Route Pattern**, and then click **Add New** in order to create a new route pattern.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Route Pattern—**861XXXX**
- Gateway/Route List—**TR1-TCS1-Record-10.106.170.177**



Pattern Definition

Route Pattern*	861XXXX
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	TR1-TCS1-Record-10.106.170.177

Step 3. Click **Save**.

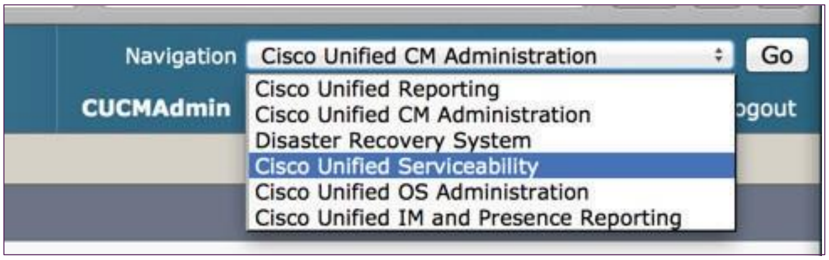
Procedure 9 Configure Unified CM SIP route pattern for personal CMR conferences

The regular Unified CM SIP route pattern routing cannot be used for routing calls to the personal CMR conferences created in this document because Unified CM can route URIs only based on domains (e.g. cisco.local) and not the URIs created for the personal CMR conferences (e.g. cmr@mmcvd.ciscolabs.com).

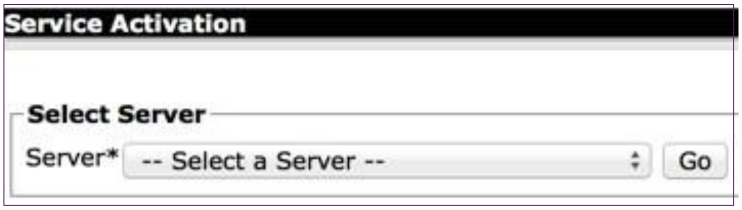
To route the calls to the personal CMR conference URIs we have to use the ILS (Intercluster Lookup Service) service in the Unified CM and manually import the personal CMR conference URIs into the Unified CM.

Following steps will configure the Unified CM to enable ILS and import the permpersonal CMR conference URLs.

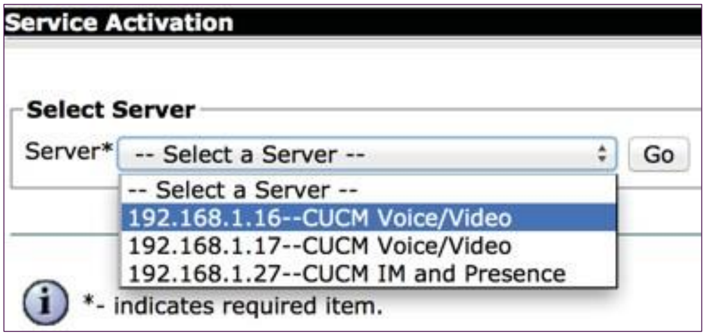
Step 1. Click the **Navigation** tab on the top right corner of the **Unified CM Administration** page, select **Cisco Unified Serviceability** from the dropdown list and click **Go**.


Navigation
Cisco Unified CM Administration
Go
CUCMAdmin
Cisco Unified Reporting
Cisco Unified CM Administration
Disaster Recovery System
Cisco Unified Serviceability
Cisco Unified OS Administration
Cisco Unified IM and Presence Reporting
ogout

Step 2. Navigate to **Tools > Service Activation**.

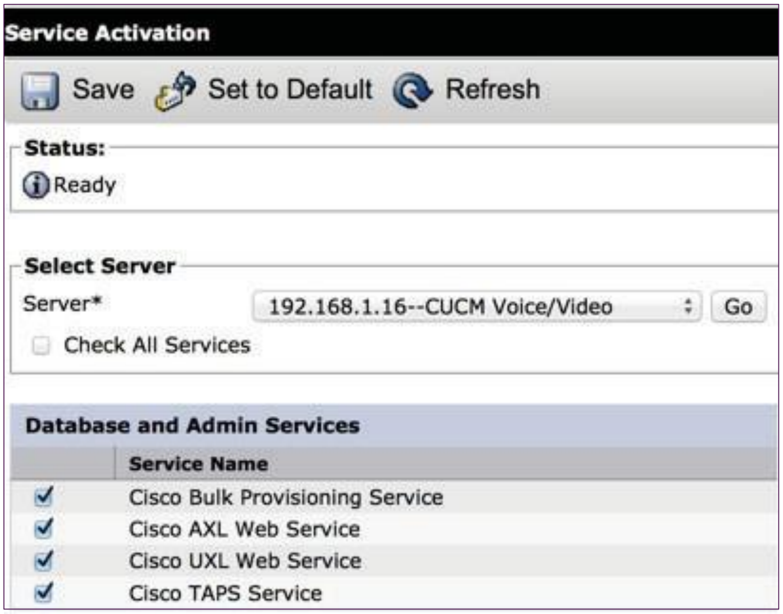


Step 3. Select **192.168.1.16–CUCM Voice/Video** from the dropdown list under **Server** and click **Go**.



Service Activation
Select Server
Server*
-- Select a Server --
Go
-- Select a Server --
192.168.1.16--CUCM Voice/Video
192.168.1.17--CUCM Voice/Video
192.168.1.27--CUCM IM and Presence
*- indicates required item.

Step 4. Select the **Cisco Bulk Provisioning Service** under the **Database and Admin Services** and click **Save**.

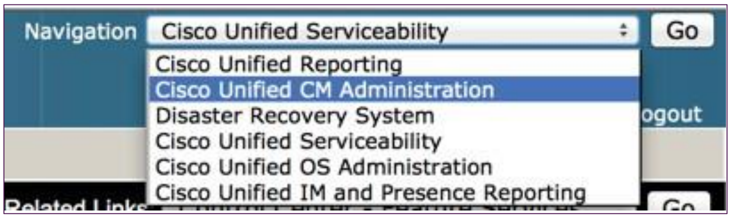


Server* 192.168.1.16--CUCM Voice/Video

□ Check All Services

	Service Name
☑	Cisco Bulk Provisioning Service
☑	Cisco AXL Web Service
☑	Cisco UXL Web Service
☑	Cisco TAPS Service

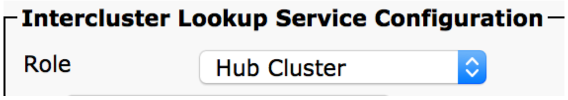
Step 5. Go back to **the Cisco Unified CM Administration** page by clicking on the **Navigation** tab on top right corner of the **Cisco Unified Serviceability** page, selecting the **Cisco Unified CM Administration** and then clicking **Go**.



Navigation
Cisco Unified Serviceability
Go
Cisco Unified Reporting
Cisco Unified CM Administration
Disaster Recovery System
Cisco Unified Serviceability
Cisco Unified OS Administration
Cisco Unified IM and Presence Reporting
ogout
Related Links
Go

ILS has to be enabled and working for the further steps to work. ILS can work either in “Hub Cluster” or “Spoke Cluster” mode. In this CVD we have a single cluster deployment so we will configure this publisher in “Hub Cluster” mode.

Step 6. Navigate to Advanced Features > ILS Configuration and select Hub Cluster as the Role under the Intercluster Lookup Service Configuration tab.



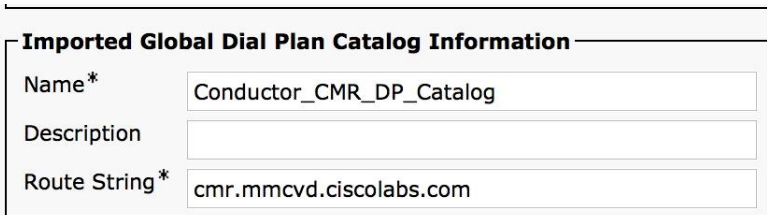
Intercluster Lookup Service Configuration

Role	Hub Cluster

Step 7. Navigate to **Call Routing > Global Dial Plan Replication > Imported Global Dial Plan Catalogue** and click Add New.

Step 8. Enter the following into the relevant fields:

- Name—Conductor_CMR_DP_Catalog
- Route String—cmr.mmcvd.ciscolabs.com



Imported Global Dial Plan Catalog Information

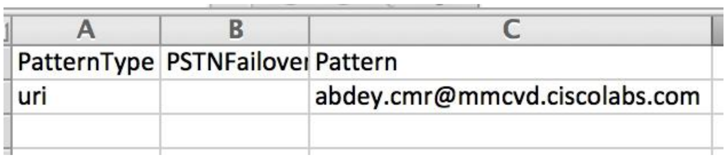
Name*	Conductor_CMR_DP_Catalog
Description	
Route String*	cmr.mmcvd.ciscolabs.com

i Tech Tip

The Route String is just a name, it does not represent that the user will have to dial *cmr.mmcvd.ciscolabs.com.

Step 9. Click Save.

Step 10. Create a cvd_cmr.csv file in the following format for all the personal CMR conference URIs that has to be imported into the ILS of the Unified CM.



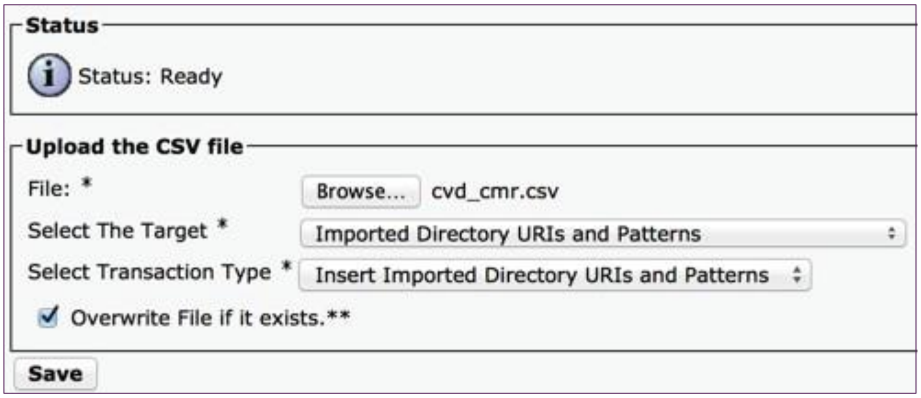
A	B	C
PatternType	PSTNFailover	Pattern
uri		abdey.cmr@mmcvd.ciscolabs.com

Step 11. Navigate to Bulk Administration > Upload/Download Files and click Add New.

Step 12. Enter the following into the relevant fields:

- File—cvd_cmr.csv
- Select The Target—Imported Directory URIs and Patterns
- Select Transaction Type—Insert Imported Directory URIs and Patterns

- Overwrite File if it exists—**Selected**



Status

Status: Ready

Upload the CSV file

File: * Browse... cvd_cmr.csv

Select The Target * Imported Directory URIs and Patterns

Select Transaction Type * Insert Imported Directory URIs and Patterns

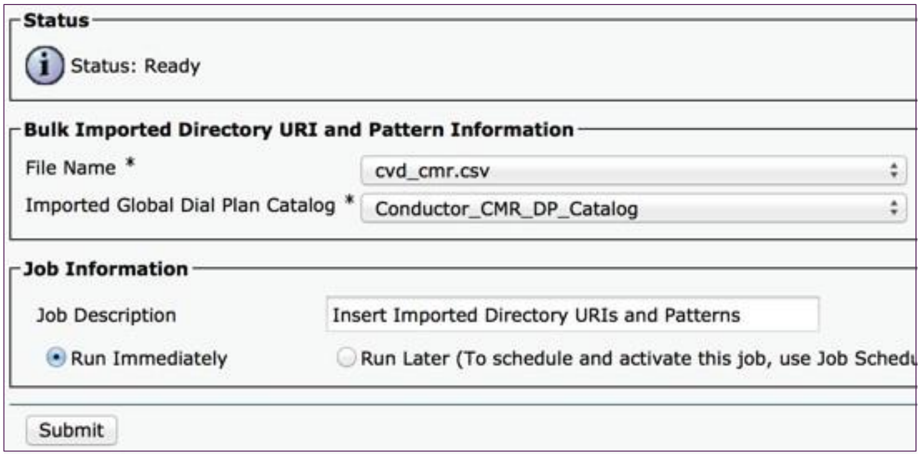
☑ Overwrite File if it exists.**

Step 13. Click **Save**.

Step 14. Navigate to **Bulk Administration > Directory URIs and Patterns > Insert Imported Directory URI and Pattern Configuration**.

Step 15. Enter the following into the relevant fields:

- File Name—**cvd_cmr.csv**
- Imported Global Dial Plan Catalog—**Conductor_CMR_DP_Catalog**
- Run Immediately—**Selected**



Status

Status: Ready

Bulk Imported Directory URI and Pattern Information

File Name * cvd_cmr.csv

Imported Global Dial Plan Catalog * Conductor_CMR_DP_Catalog

Job Information

Job Description Insert Imported Directory URIs and Patterns

● Run Immediately ○ Run Later (To schedule and activate this job, use Job Schedu

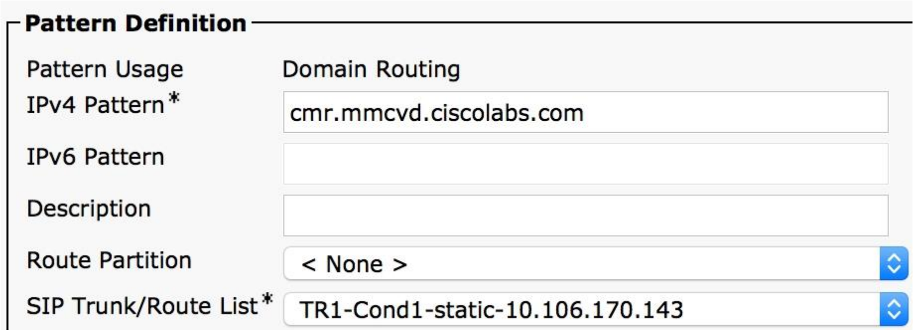
Step 16. Click **Submit**.

Step 17. Navigate to **Call Routing > SIP Route Pattern**.

Step 18. Click **Add New**.

Step 19. Enter the following into the relevant fields, leaving other fields at their default values:

- IPv4 Pattern—**cmr.mmcvd.ciscolabs.com**
- SIP Trunk/Route List—**TR1-Cond1-static-10.106.170.143**



Pattern Definition

Pattern Usage	Domain Routing
IPv4 Pattern*	cmr.mmcvd.ciscolabs.com
IPv6 Pattern	
Description	
Route Partition	< None >
SIP Trunk/Route List*	TR1-Cond1-static-10.106.170.143

Step 20. Click **Save**.

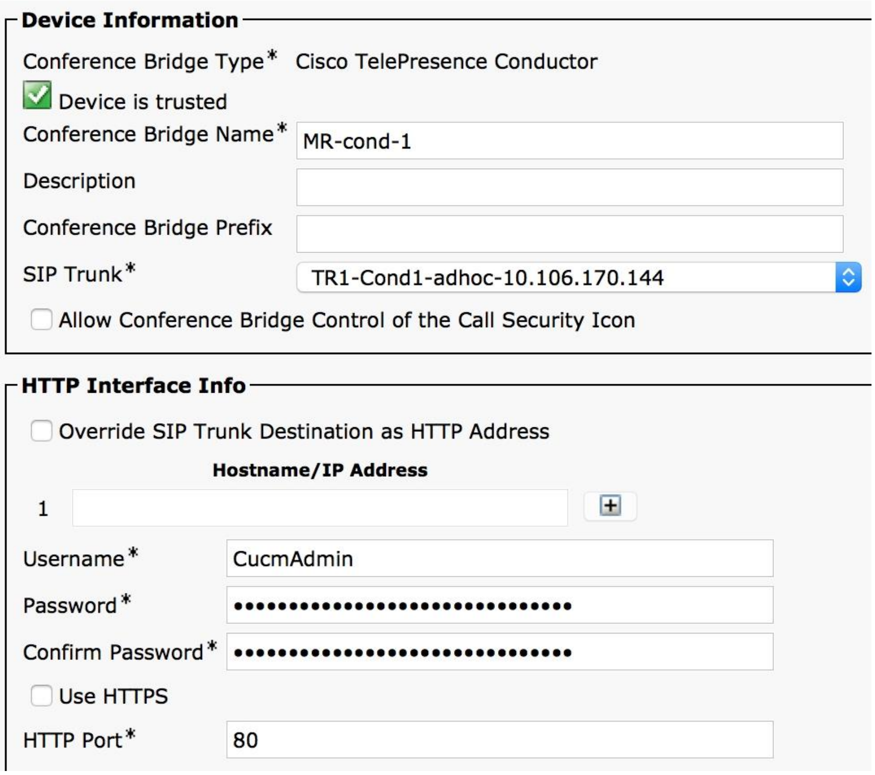
Procedure 10 Configure Conductor as conference bridge

This procedure describes configuring Conductor as a conference bridge in Unified CM for instant CMR conferences.

Step 1. Navigate to **Media Resources > Conference Bridge**, and then click **Add New** in order to create a new conference bridge.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Conference Bridge Type—**Cisco TelePresence Conductor**
- Conference Bridge Name—**MR-cond-1**
- SIP Trunk—**TR1-Cond1-adhoc-10.106.170.144**
- Allow Conference Bridge Control of the Call Security Icon—**UnSelected**
- Override SIP Trunk Destination as HTTP Address—**UnSelected**
- Username—**CucmAdmin**
- Password—**<password for CucmAdmin created in Conductor>**
- HTTP Port—**80**



Device Information

Conference Bridge Type* Cisco TelePresence Conductor

☑ Device is trusted

Conference Bridge Name* MR-cond-1

Description

Conference Bridge Prefix

SIP Trunk* TR1-Cond1-adhoc-10.106.170.144

□ Allow Conference Bridge Control of the Call Security Icon

HTTP Interface Info

□ Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1

Username* CucmAdmin

Password* ••••••••••••••••••••••••••••••

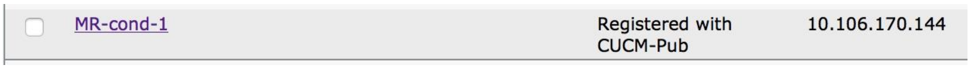
Confirm Password* ••••••••••••••••••••••••••••••

□ Use HTTPS

HTTP Port* 80

Step 3. Click **Save**.

Step 4. Make sure that the Conference Bridge shows as registered to the Unified CM.



□	MR-cond-1	Registered with CUCM-Pub	10.106.170.144

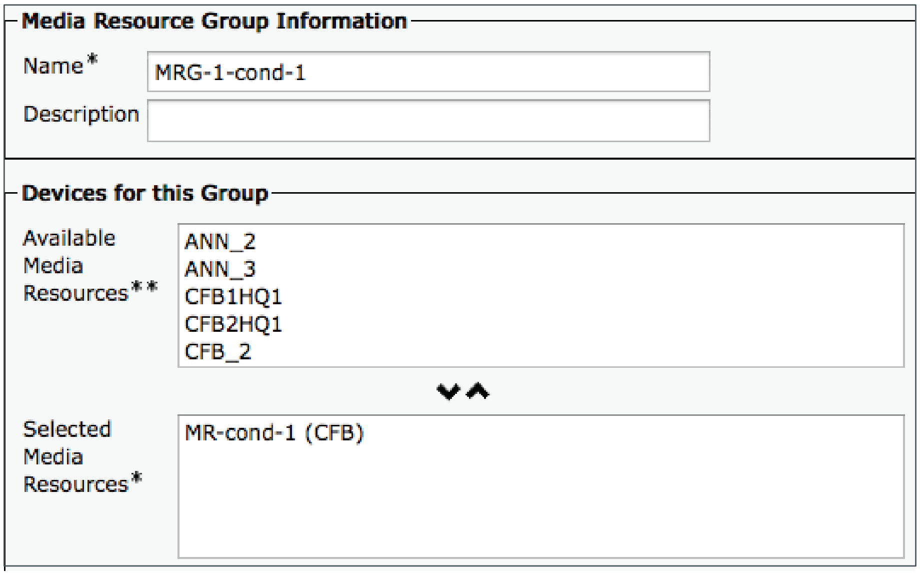
Procedure 11 Configure MRG and MRGL for video and add Conductor to this MRG

Step 1. Navigate to Media Resources > Media Resource Group, and then click Add New.

Step 2. In Name, enter **MRG-1-cond-1**.

Step 3. In Available Media Resources, select MR-cond-1 (CFB) and click the down arrow to move it down to the Selected Media Resources.

Step 4. Click Save.



Media Resource Group Information

Name* MRG-1-cond-1

Description

Devices for this Group

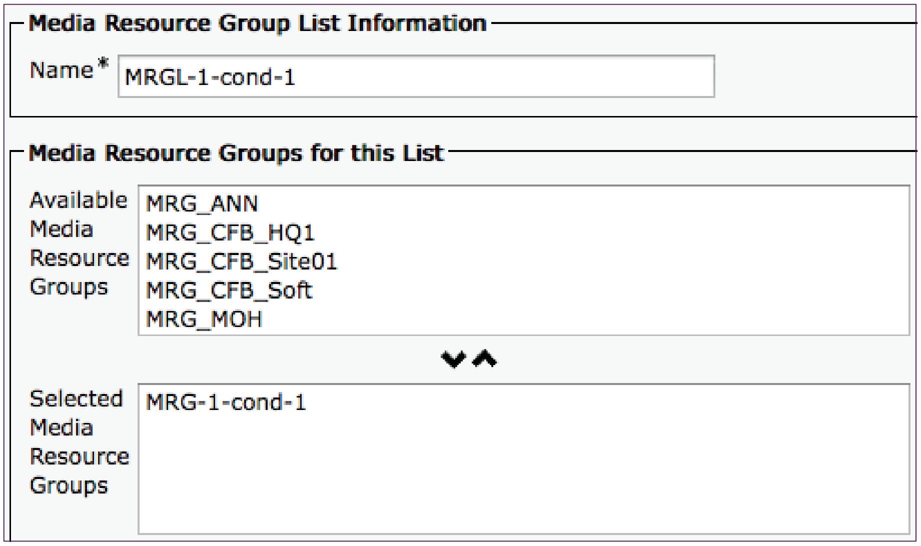
Available Media Resources**
ANN_2
ANN_3
CFB1HQ1
CFB2HQ1
CFB_2

Selected Media Resources* MR-cond-1 (CFB)

Step 5. Navigate to Media Resources > Media Resource Group List, and then click Add New.

Step 6. In Name, enter **MRGL-1-cond-1**

Step 7. In **Available Media Resources Groups**, select **MRG-1-cond-1** and click the down arrow to move it down to the **Selected Media Resources Groups**.



Media Resource Group List Information

Name* MRGL-1-cond-1

Media Resource Groups for this List

Available Media Resource Groups: MRG_ANN, MRG_CFB_HQ1, MRG_CFB_Site01, MRG_CFB_Soft, MRG_MOH

Selected Media Resource Groups: MRG-1-cond-1

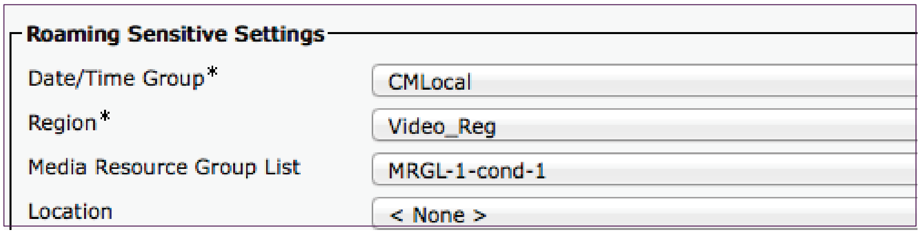
Step 8. Click **Save**.

Procedure 12 Add this MRGL to the device profile for video

Step 1. Navigate to **System > Device Pool**, and then click **Find** in order to list all configured Device Pools.

Step 2. Select **Video_DP**.

Step 3. In **Media Resource Group List**, select **MRGL-1-cond-1**.



Roaming Sensitive Settings

Date/Time Group*	CMLocal
Region*	Video_Reg
Media Resource Group List	MRGL-1-cond-1
Location	< None >

Step 4. Click **Save**.

Configuring Cisco TelePresence Content Server

PROCESS

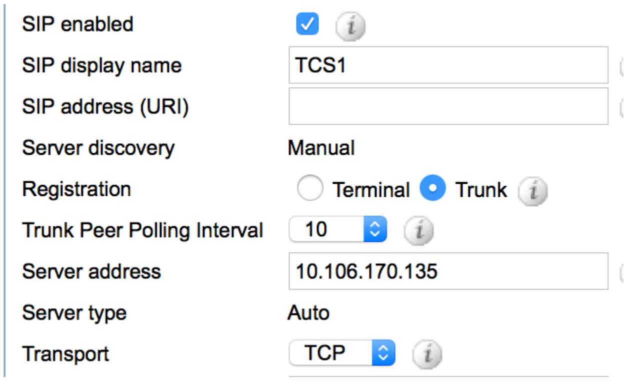
1. Configure Site settings (recording only)
2. Configure Recording Alias (recording only)

Procedure 1 Configure Site settings (recording only)

Step 1. Navigate to **Configuration > Site settings**.

Step 2. In SIP settings, enter the following in the relevant fields:

- SIP enabled – **checked**
- SIP display name – **TCS1**
- Registration – **Trunk**
- Server Address – **10.106.170.135**
- Transport **TCP**



SIP enabled	☑
SIP display name	TCS1
SIP address (URI)	
Server discovery	Manual
Registration	○ Terminal ● Trunk
Trunk Peer Polling Interval	10
Server address	10.106.170.135
Server type	Auto
Transport	TCP

Step 3. Click **Save**.

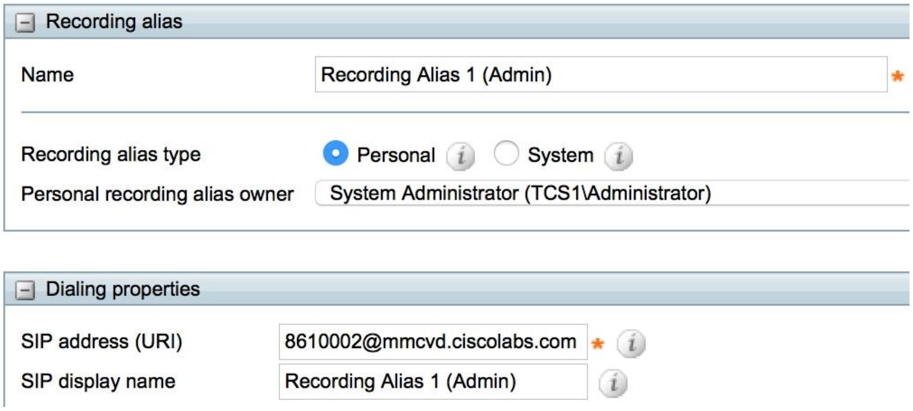
Procedure 2 Configure Recording Alias (recording only)

Step 1. Navigate to **Recording setup > Recording Aliases** and click **Add Recording Alias**.

Step 2. Enter the following in the relevant fields and leave the other fields at their default values:

- Name – **Recording Alias 1 (Admin)**

- SIP address (URI) - **8610002@mmcvd.ciscolabs.com**



Recording alias

Name	Recording Alias 1 (Admin) *
Recording alias type	● Personal ○ System
Personal recording alias owner	System Administrator (TCS1\Administrator)

Dialing properties

SIP address (URI)	8610002@mmcvd.ciscolabs.com *
SIP display name	Recording Alias 1 (Admin)

Step 3. Click **Save**.

Configuring Endpoints

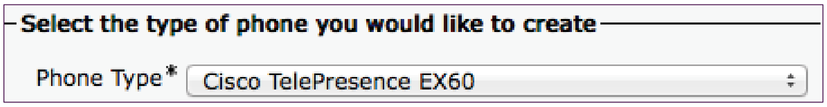
PROCESS

1. Configure Unified CM for endpoints
2. Configure SX20

Procedure 1 Configure Unified CM for endpoints

Step 1. Navigate to **Device > Phone**, and then click **Add New**.

Step 2. In **Phone Type**, select **Cisco TelePresence EX60**, and then click **Next**:



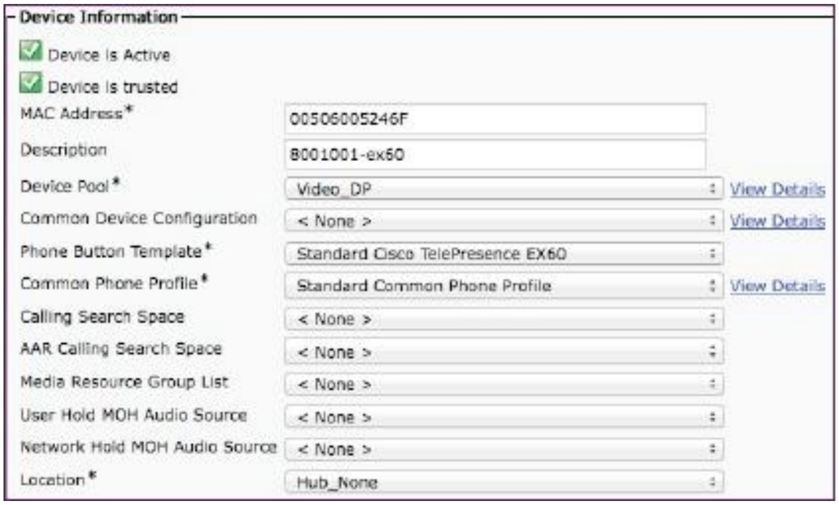
Select the type of phone you would like to create

Phone Type* Cisco TelePresence EX60

Step 3. Click **Next**.

Step 4. Enter the following into the relevant field, leaving the other fields at their default values:

- MAC Address–**00506005246F**
- Device Pool–**Video_DP**
- Phone Button Template–**Standard Cisco TelePresence EX60**
- Common Phone Profile–**Standard Common Phone Profile**
- Device Security Profile–**Cisco TelePresence EX60–Standard**
- SIP Profile–**Standard SIP Profile for TelePresence Endpoint**

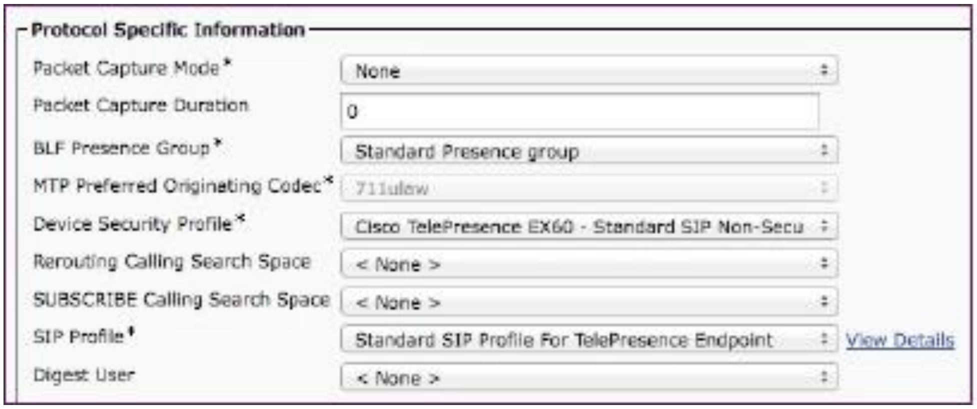


Device Information

☑ Device is Active

☑ Device is trusted

MAC Address*	00506005246F	
Description	8001001-ex60	
Device Pool*	Video_DP	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Standard Cisco TelePresence EX60	
Common Phone Profile*	Standard Common Phone Profile	View Details
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	

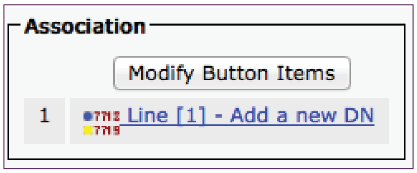


Protocol Specific Information

Packet Capture Mode*	None	
Packet Capture Duration	0	
BLF Presence Group*	Standard Presence group	
MTP Preferred Originating Codec*	711ulaw	
Device Security Profile*	Cisco TelePresence EX60 - Standard SIP Non-Secu	
Rerouting Calling Search Space	< None >	
SUBSCRIBE Calling Search Space	< None >	
SIP Profile*	Standard SIP Profile For TelePresence Endpoint	View Details
Digest User	< None >	

Step 5. Click **Save**.

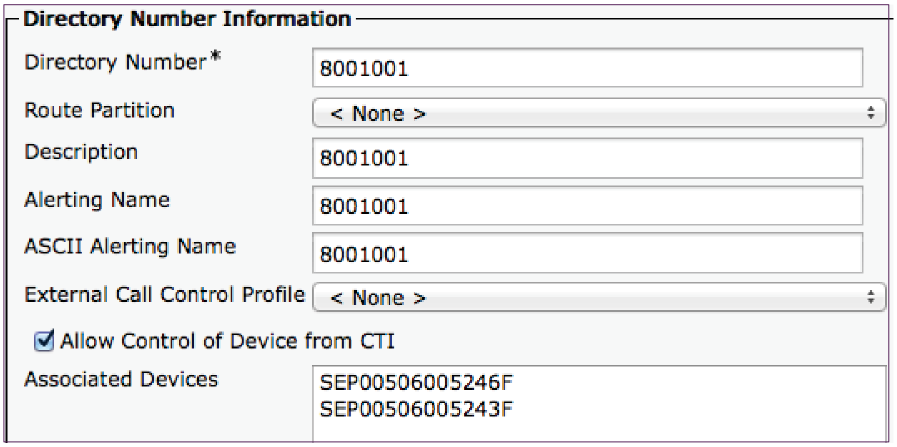
Step 6. Click **Line [1]–Add a new DN**.



Association

1	Line [1] - Add a new DN

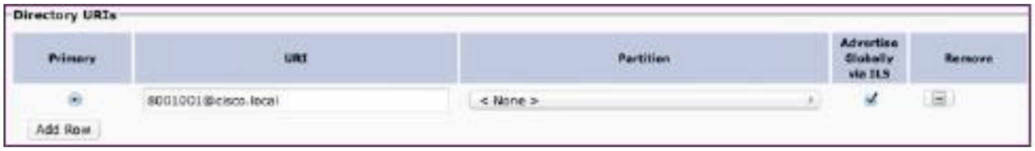
Step 7. In **Directory Number**, enter **8001001**, and then click **Save**.



Directory Number Information

Directory Number*	8001001
Route Partition	< None >
Description	8001001
Alerting Name	8001001
ASCII Alerting Name	8001001
External Call Control Profile	< None >
☑ Allow Control of Device from CTI	
Associated Devices	SEP00506005246F SEP00506005243F

Step 8. Under **Directory URIs**, enter **8001001@cisco.local** as the URI and click **Add Row**.



Directory URIs

Primary	URI	Partition	Advertise Globally via ILS	Remove
●	8001001@cisco.local	< None >	✓	⊟

Procedure 2 Configure SX20

Step 1. Navigate to **Home > Settings > Administrator Settings > Advanced Configuration > Provisioning > External Manager > Address**.

Step 2. In **External Manager**, enter **10.106.170.135**, and then click **Save**.

Recording Self Video

PROCESS

1. Dial TCS URI (recording only)

Procedure 1 Dial TCS URI (recording only)

Step 1. Dial **8610002@mmcvd.ciscolabs.com** and wait till the countdown finishes and is 0.

Now the call to the TCS will be recording till the call is put to an end.

Initiating Conferences

PROCESS

1. Initiate instant CMR conference
2. Create Personal CMR conferences
3. Initiate Personal CMR conference
4. Create scheduled CMR conference

Procedure 1 Initiate instant CMR conference

Step 1. Call **8001002** from **8001001**.

Step 2. After the call is connected, press on the **Add+** button.

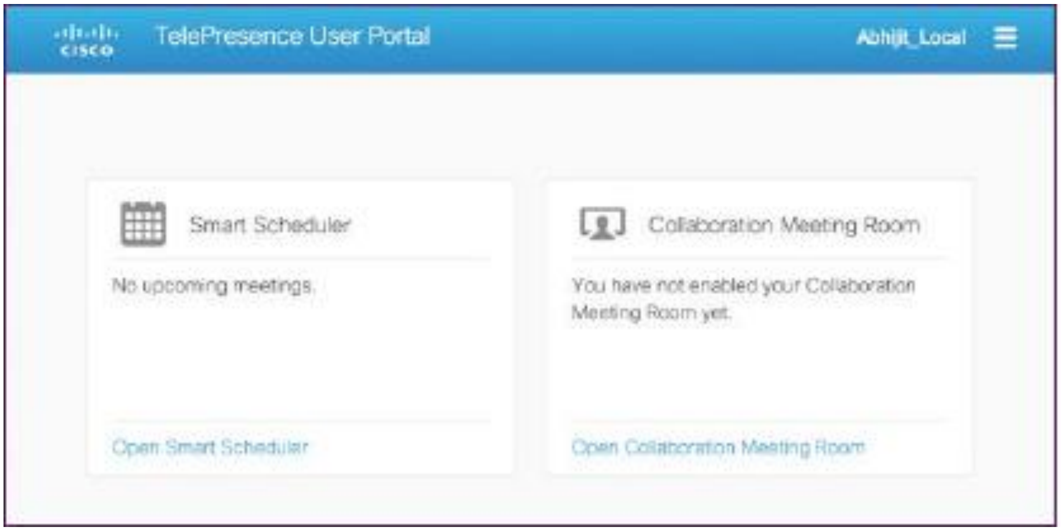
Step 3. Call **8001003** from **8001001**.

Step 4. Press the **Merge** button.

The instant CMR conference should be connected.

Procedure 2 Create Personal CMR conferences

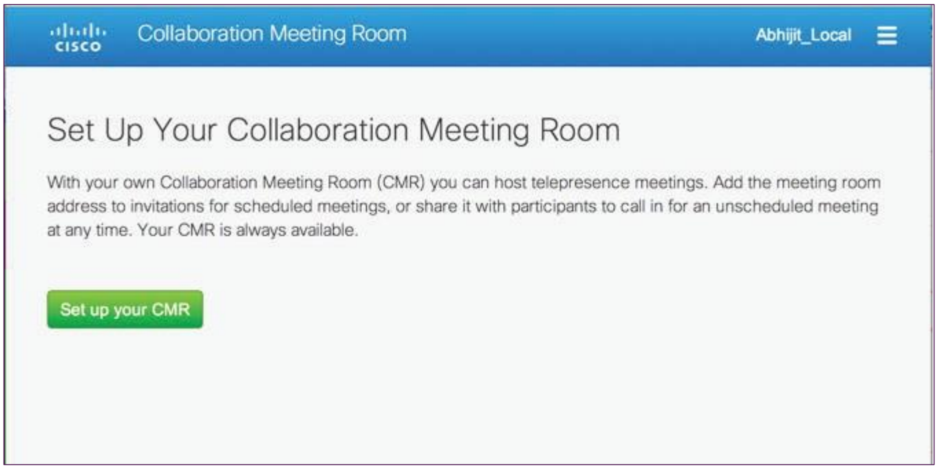
Step 1. Open a browser, type **https://10.106.170.153/tmsagent/tmsportal/#home** in the navigation space and click **Go**.



No upcoming meetings.

You have not enabled your Collaboration Meeting Room yet.

Step 2. Click on **Open Collaboration Meeting Room**.

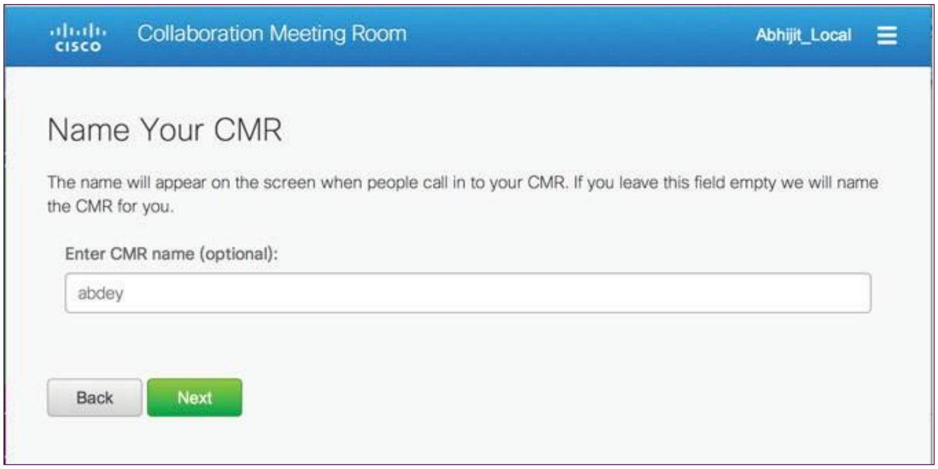


Set Up Your Collaboration Meeting Room

With your own Collaboration Meeting Room (CMR) you can host telepresence meetings. Add the meeting room address to invitations for scheduled meetings, or share it with participants to call in for an unscheduled meeting at any time. Your CMR is always available.

Step 3. Click **Set up your CMR**.

Step 4. Enter the personal CMR **conference** name as **abdey** and click **Next**.

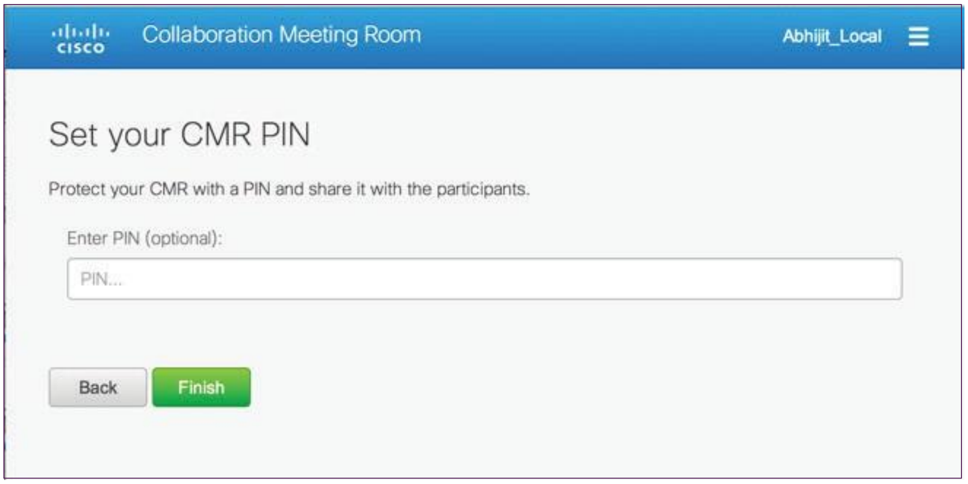


Name Your CMR

The name will appear on the screen when people call in to your CMR. If you leave this field empty we will name the CMR for you.

Enter CMR name (optional): abdey

Step 5. On the Set your **CMR PIN page**, click **Finish**.

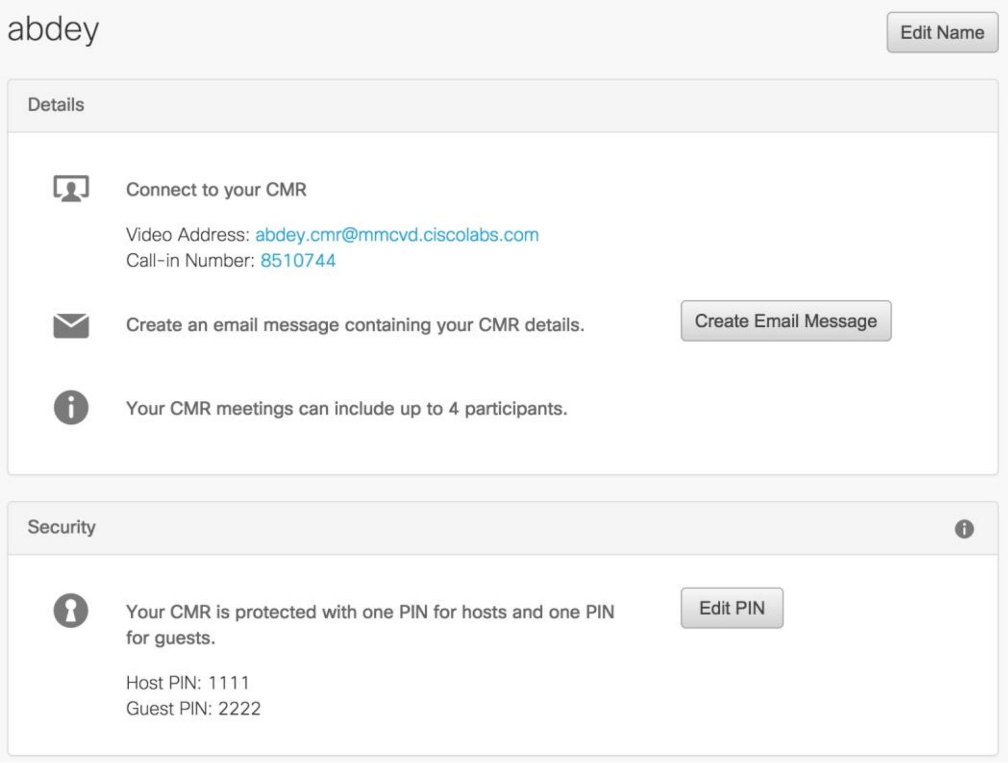


Set your CMR PIN

Protect your CMR with a PIN and share it with the participants.

Enter PIN (optional):

PIN...



abdey

Details

Connect to your CMR

Video Address: abdey.cmr@mmcvd.ciscolabs.com
Call-in Number: 8510744

Create an email message containing your CMR details.

Your CMR meetings can include up to 4 participants.

Security

Your CMR is protected with one PIN for hosts and one PIN for guests.

Host PIN: 1111
Guest PIN: 2222

The Personal CMR conference is created.

Procedure 3 Initiate Personal CMR conference

Step 1. Call **abdey.cmr@mmcvd.ciscolabs.com** from **8001001**.

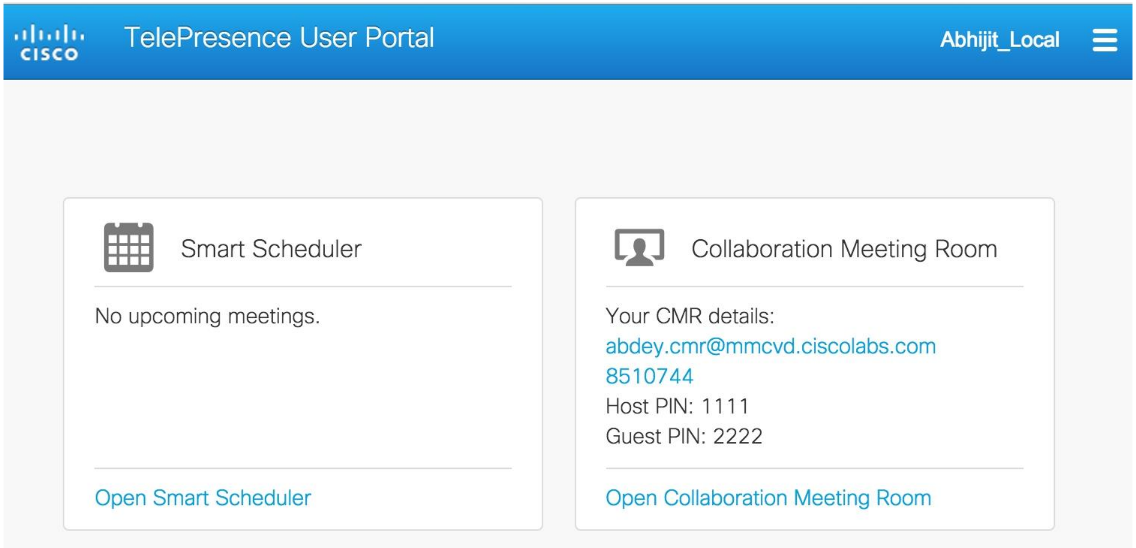
Step 2. Call **abdey.cmr@mmcvd.ciscolabs.com** from **8001003**.

Step 3. Call **abdey.cmr@mmcvd.ciscolabs.com** from **8001003**.

The personal CMR conference should be connected.

Procedure 4 Create scheduled CMR conference

Step 1. Open a browser, type **https://10.106.170.153/tmsagent/tmsportal/#home** in the navigation space and click **Go**.



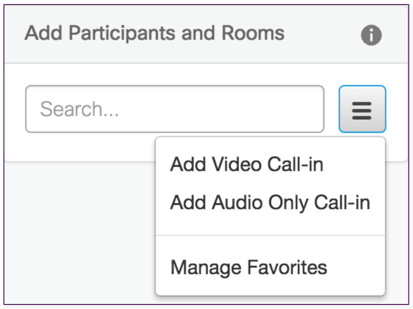
No upcoming meetings.

Your CMR details:
abdey.cmr@mmcvd.ciscolabs.com
8510744
Host PIN: 1111
Guest PIN: 2222

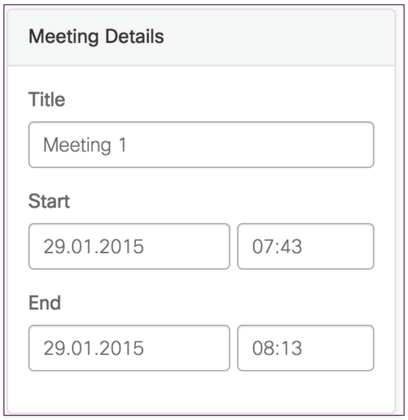
Step 2. Click **Open Smart Scheduler**.

Step 3. Click **New Meeting**.

Step 4. Add Video and/or audio Call-in.



Step 5. Enter **Meeting 1** as Title.



Meeting Details

Title: Meeting 1

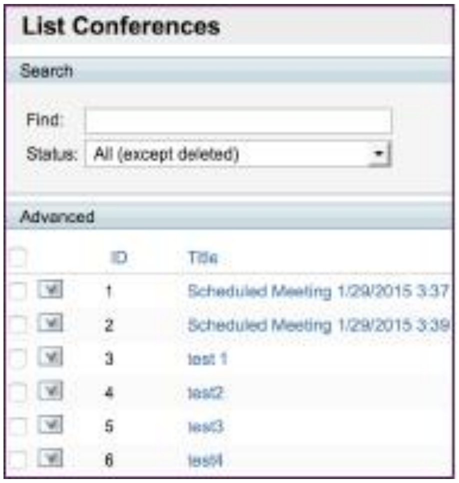
Start: 29.01.2015 07:43

End: 29.01.2015 08:13

Step 6. Click **Save**.

Step 7. Open a new browser, type **https://10.106.170.153/tms/** in the navigation space and click **Go**.

Step 8. Navigate to **Booking > List Conferences**.



List Conferences

Search

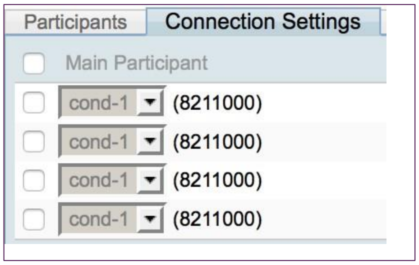
Find:

Status: All (except deleted)

Advanced

□		ID	Title
□	☑	1	Scheduled Meeting 1/29/2015 3:37
□	☑	2	Scheduled Meeting 1/29/2015 3:39
□	☑	3	test 1
□	☑	4	test2
□	☑	5	test3
□	☑	6	test4

Step 9. Click **Meeting 1**.



□ Main Participant

□ cond-1 ▾ (8211000)

□ cond-1 ▾ (8211000)

□ cond-1 ▾ (8211000)

□ cond-1 ▾ (8211000)

Step 10. Click on **Connection Settings** tab.

The number displayed in braces is the scheduled CMR conference dial-in number that the users have to dial at the scheduled time.

Recording Instant CMR Conferences

PROCESS

1. Join TCS as an instant CMR conference participant (recording only)

Procedure 1 Join TCS as an instant CMR conference participant (recording only)

Step 1. In the instant CMR conference, click on the **Add** button and dial **8610002@mmcvd.ciscolabs.com** and wait till the countdown finishes and is 0.

Step 2. Click the **Merge** button.

Now the call to the TCS will be recording till the call is put to an end.

Appendix A: Product List

Component	Product Description	Part Number	Software
Call Control	Cisco Unified CM Business Edition 6000 with up to 1000 users	BE6H-M4-K9= BE6H-M4-XU=	11.0(1)
Video Phones	Unified IP Phones 8800 series	CP-88xx-K9=	10.3.1
	Unified IP Phones DX650	CP-DX650-K9	10.2.4
Video Endpoints	Cisco TelePresence DX70	CP-DX70-W-K9=	10.2.4
	Cisco TelePresence DX80	CP-DX80-K9=	10.2.4
	Cisco TelePresence SX10	CTS-SX10-K9	TC7.3.3
	Cisco TelePresence SX20	CTS-SX20-PHD2.5X-K9	TC7.3.3
Conference Bridge Controller	Mid Market Virtual TelePresence Conductor	R-VMCNDTRM-K9	4.0
	Cisco TelePresence Management Suite	CTI-TMS-SW-K9	15.0
	Cisco TelePresence Management Suite Provisioning Extension		1.5
Video Conference Bridge	Virtual TelePresence Server	R-VTS-K9	4.2
Video Recording Server	Cisco TelePresence Content Server	BE6K-VMTCS-1R-1L	6.2
Soft Client	Cisco Jabber for Windows	JAB9-DSK-K9	11.0

Feedback

Please send comments and suggestions about this guide to collab-mm-cvd@external.cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.**

Printed in USA

CXX-XXXXXX-XX 09/15