



Video Conferencing & Recording Using Cisco BE6000

Cisco Validated Design Guide

August 2016

© 2016 Cisco Systems, Inc. All rights reserved.





Contents

Preface.....	3
Scope	3
Proficiency	4
Comments and Questions	4
Disclaimer	4
Introduction	5
Technology Use Case	5
Use Case: Video Collaboration with Desktop and Multipurpose Room Systems.....	5
Design Overview	6
Cisco Preferred Architecture.....	6
Network Considerations	7
Solution Details	7
Cisco Unified Communications Manager	9
Cisco Video and TelePresence Endpoints.....	9
Cisco TelePresence Server on Virtual Machine.....	9
Cisco TelePresence Conductor	9
Cisco TelePresence Management Suite	10
Cisco TelePresence Content Server	10
Dial Plan.....	10
Deployment Details.....	12
Installing TelePresence Server	13
Installing TelePresence Conductor	19
Installing TelePresence Management Suite (TMS) and TelePresence Management Suite Provisioning Extension (TMSPE).....	23
Installing Cisco TelePresence Content Server	38
Configuring Cisco TelePresence Server	44
Configuring Cisco TelePresence Conductor.....	46
Configuring Cisco TelePresence Management Suite (TMS)	65
Configuring Cisco Unified Communications Manager (Unified CM)	75
Configuring Cisco TelePresence Content Server	92
Configuring Endpoints	95
Recording Self Video.....	98
Initiating Conferences.....	99
Recording Instant CMR Conferences	105
Appendix A: Product List.....	106

[Content](#)[Technology Use Case](#)[Design Overview](#)[Deployment Details](#)[Product List](#)

Preface

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.

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

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.

This document details **Video Collaboration with Desktop and Multipurpose Room Systems**. It 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 technical proficiencies—or equivalent experience in CCNA Collaboration—1 to 3 years in designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Comments and Questions

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

Disclaimer

The IP address scheme used in this document is for representational purposes only.



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

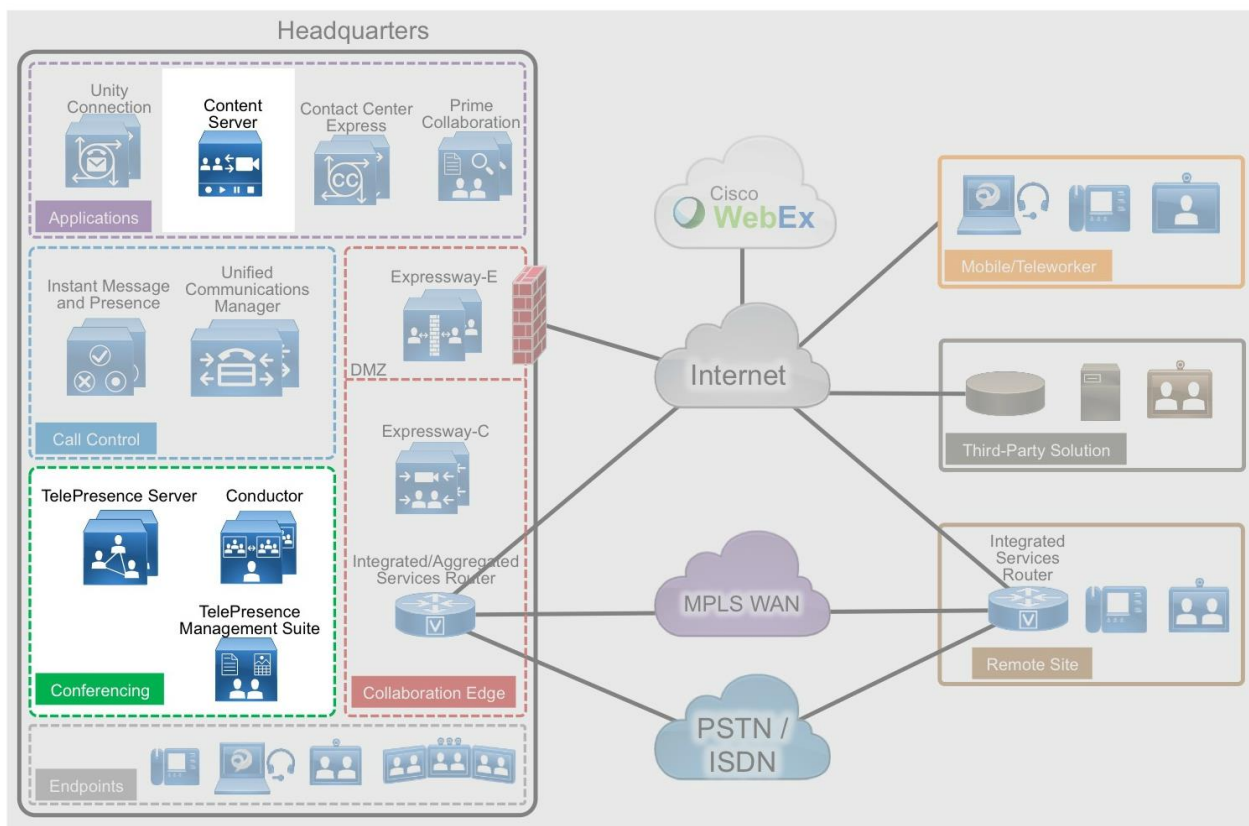
An end-to-end video-collaboration solution incorporates a full suite of endpoints, infrastructure components, and centralized management tools.

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.

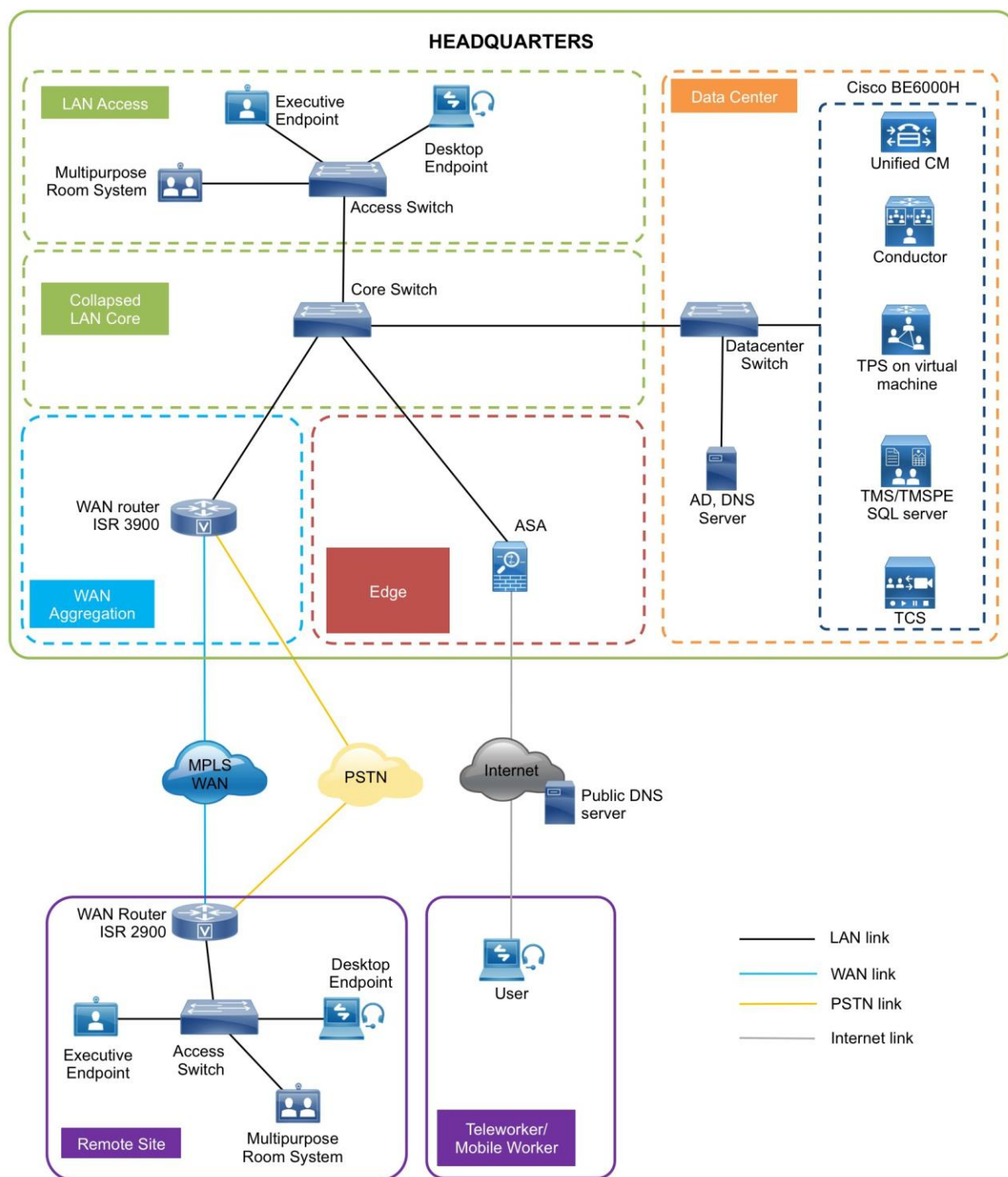
With an IP network, the ongoing costs of running video calls are minimal because you only have to pay for maintenance and technical support. When return on investment (ROI) for the initial deployment is met, any additional costs are essentially free. Because there is no incremental cost involved, employees 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 always-on virtual spaces that have a fixed video address. Users can call in to that address at any time to start a meeting. Creation of a CMR requires deployment of a TelePresence Conductor with a Unified CM, configured with one or more conference bridge pools and Service Preferences. TMS and TMSPE are 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 number, from a configured range in TMS, 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 Unified CM. For self-video recording the user has to dial a preconfigured 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**


[Content](#)
[Technology Use Case](#)
[Design Overview](#)
[Deployment Details](#)
[Product List](#)

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 procedures 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 to the Installing the Cisco Unified CM process in the [Installation Guide for Cisco Business Edition 6000](#).

Easy Access Configuration Sheet

General Networking Parameters		
Element	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		
Element	CVD Configuration	Site-Specific Configuration
TelePresence Server Name	vTS3	
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		
Element	CVD Configuration	Site-Specific Configuration
User for Conductor to log in to TPS	CondAdmin	
User for TMS to log in to TPS	TMSAdmin	

PROCESS

1. [Configure Cisco Business Edition 6000 Connectivity to LAN](#)
2. [Deploy OVA to Host](#)
3. [Configure the VM Guest](#)
4. [Apply Licenses on Telepresence Server](#)

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
```

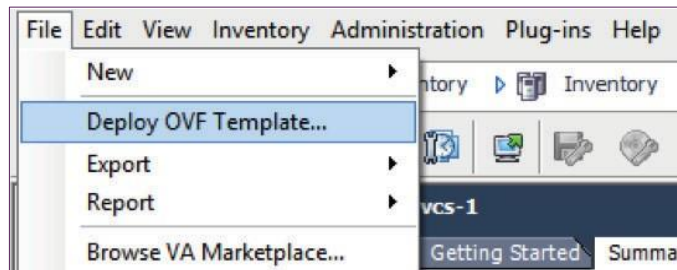
Procedure 2

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

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 **vTS3** 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**.

[Source](#)

[OVF Template Details](#)

[Name and Location](#)

Deployment Configuration

[Disk Format](#)

[Network Mapping](#)

[Ready to Complete](#)

Configuration:

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**.



Content | Technology Use Case | Design Overview | Deployment Details | Product List

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

<p>Source</p> <p>OVF Template Details</p> <p>Name and Location</p> <p>Deployment Configuration</p> <p>Disk Format</p> <p>Ready to Complete</p>	<p>Datstore: <input type="text" value="datastore1 (1)"/></p> <p>Available space (GB): <input type="text" value="3429.8"/></p> <p><input checked="" type="radio"/> Thick Provision Lazy Zeroed</p> <p><input type="radio"/> Thick Provision Eager Zeroed</p> <p><input type="radio"/> Thin Provision</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 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>i</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>i</i>	Tech Tip
----------	----------

Change the admin account to use a new password as soon as possible. Go to the Login information page, and click **Change Password**.

The VM guest is configured.

Procedure 4	Apply License on the TelePresence Server
--------------------	------------------------------------------

For the scenarios covered in this CVD, the following type of licenses can be installed on the TelePresence Server:

- Virtual Machine Activation key
- Media Encryption Key

<i>i</i>	Tech Tip
----------	----------

For additional licensing details, refer to 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 **Configuration > Upgrade**.

Step 3. On the Feature Management section, enter the following, and then click Add key:

- Virtual machine activation key in the **Add key** field
- Media encryption key in the **Add key** field



The required licenses are applied.



Installing TelePresence Conductor

Easy Access Configuration Sheet

Cisco TelePresence Conductor Installation Requirements		
Element	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		
Element	CVD Configuration	Site-Specific Configuration
User for Unified CM 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	Cond-1	
IP address for Conductor (management)	10.106.170.139	
IP address for TelePresence Conductor (instant CMR conferences)	10.106.170.143	
IP address for TelePresence Conductor (scheduled & personal CMR conferences)	10.106.170.144	

PROCESS

1. [Deploy OVA to Host](#)
2. [Configure the VM Guest](#)
3. [Apply Licenses on the 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>i</i>	Tech Tip
----------	-----------------

<p>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.</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

- 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>i</i>	Tech Tip
----------	-----------------

<p>Because VM performance may degrade during the resizing of a partition, Thin Provision is not recommended.</p>	
------------------------------------------------------------------------------------------------------------------	--

- 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 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.

The VM guest is configured.

[Content](#)[Technology Use Case](#)[Design Overview](#)[Deployment Details](#)[Product List](#)**Procedure 3**

Apply Licenses on the 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

**Tech Tip**

For additional licensing details, refer the [Cisco Preferred Architecture for Midmarket Collaboration Design Overview](#).

- Step 7.** In your browser, enter the correct IP address and log in as admin.
- Step 8.** Navigate to **Maintenance > Option keys**.
- Step 9.** On the Option Keys page enter the release key provided in the **Release key** field and then click **Set release key**.
- Step 10.** On the Options Keys page, under Multiparty Licensing section, set the **Multiparty Licensing for TelePresence Servers** as **Enabled** and click **Save**.
- Step 11.** For each option key provided, in the **Add option key** field, enter the option key value and then click **Add option**.

The required licenses are applied.



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

Easy Access Configuration Sheet

Cisco TMS Installation Requirements		
Element	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		
Element	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 a 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.

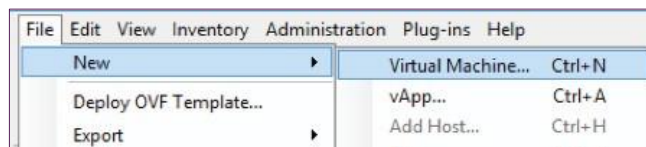
<i>i</i>	Tech Tip
	The SQL Server can also be installed off-box for resiliency.

Procedure 1

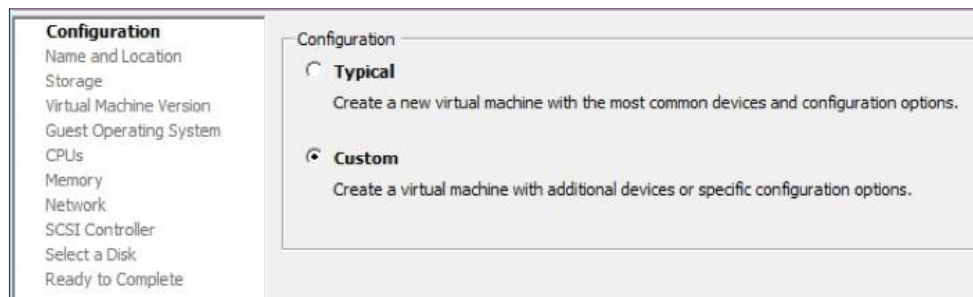
Install Windows Server

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

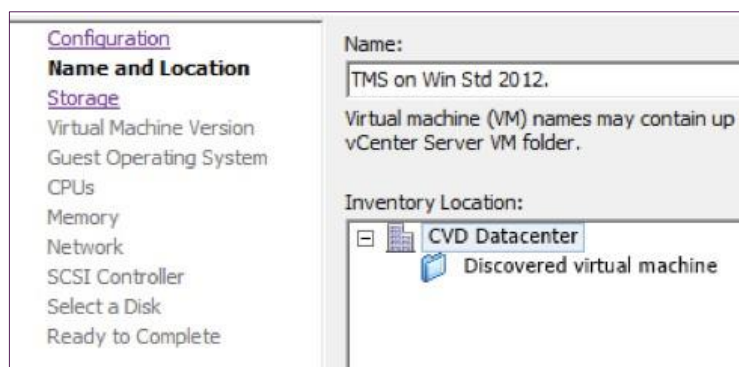
Step 2. Select **File > New > Virtual Machine**.



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



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



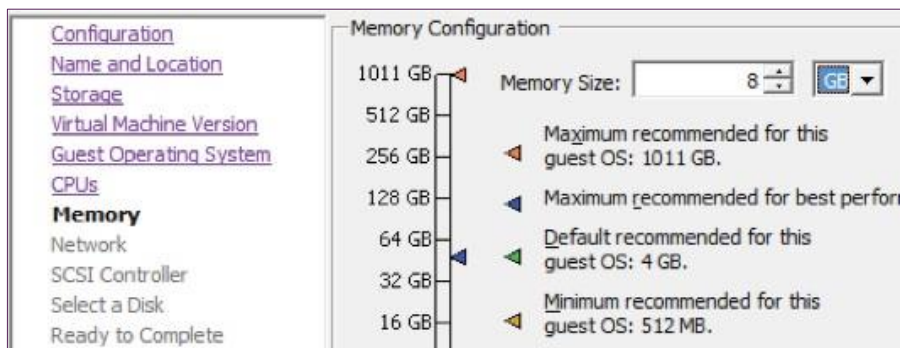
Step 5. On the Storage page select the datastore and click **Next**.

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

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

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**.

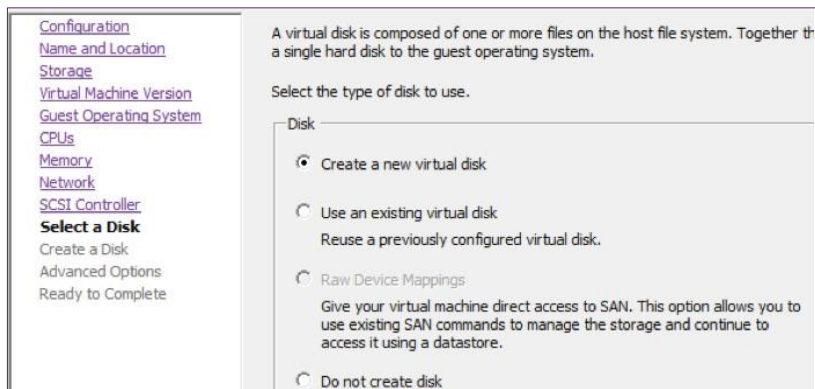
Step 9. On the Memory page, select Memory Size as **8 GB** and click **Next**.



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**.





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

The screenshot shows the 'Create a Disk' configuration interface. On the left, there is a navigation menu with links for Configuration, Name and Location, Storage, Virtual Machine Version, Guest Operating System, CPUs, Memory, Network, SCSI Controller, Select a Disk, Create a Disk, Advanced Options, and Ready to Complete. The 'Create a Disk' section is active. The main configuration area is divided into three sections: Capacity, Disk Provisioning, and Location. In the Capacity section, 'Disk Size' is set to 60 GB. In the Disk Provisioning section, 'Thick Provision Lazy Zeroed' is selected with a radio button. In the Location section, 'Store with the virtual machine' is selected with a radio button.

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.



Content | Technology Use Case | Design Overview | **Deployment Details** | Product List

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.

The Windows server is installed.

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

i 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.

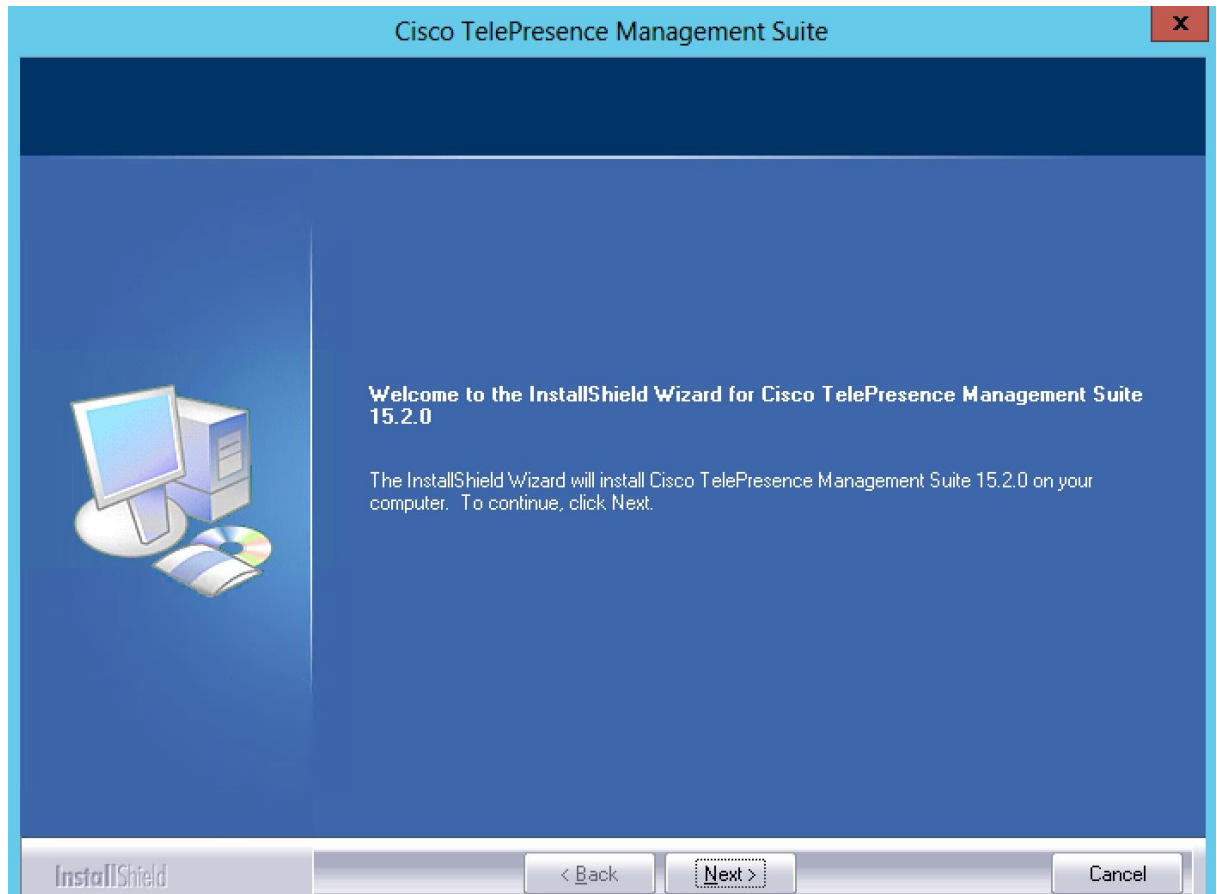
Step 3. Run the Cisco TMS executable as administrator.

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.

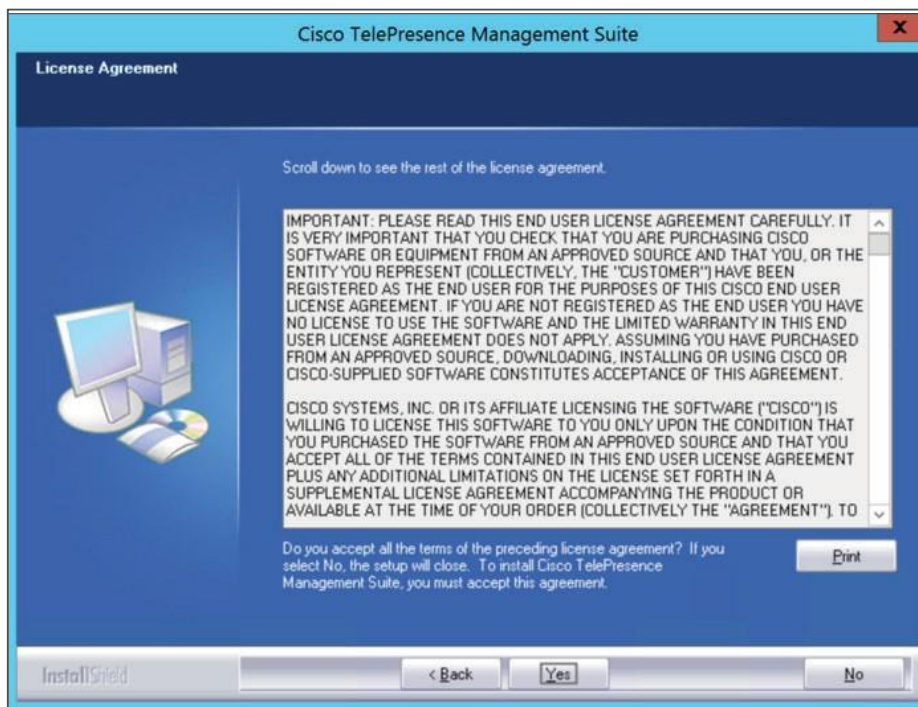
Step 4. Click **Yes** to continue.



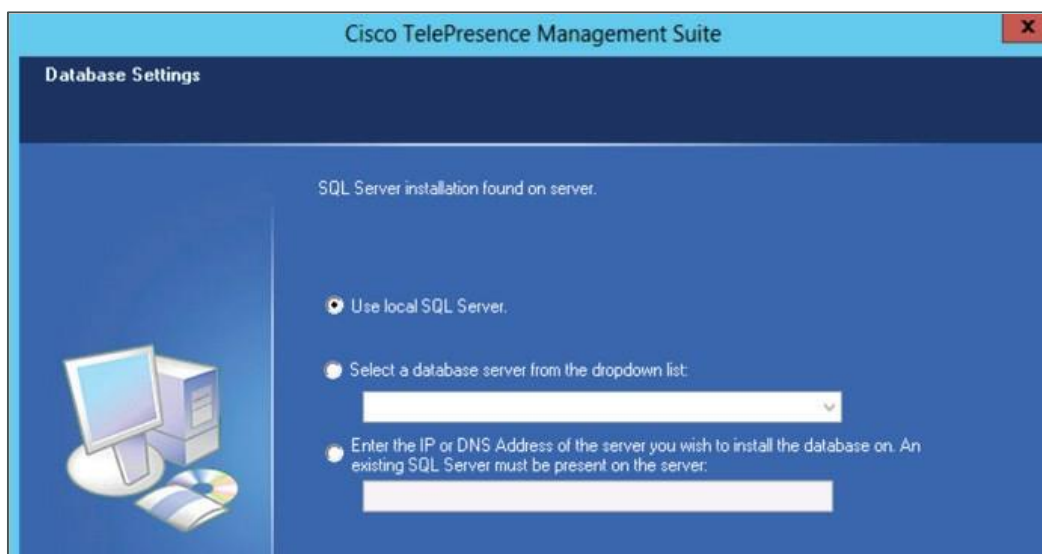
Step 5. On the welcome screen, click **Next**.



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



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**.





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

Username:

Password:

InstallShield

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.

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.

InstallShield

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**

Step 10. Click **Next**.

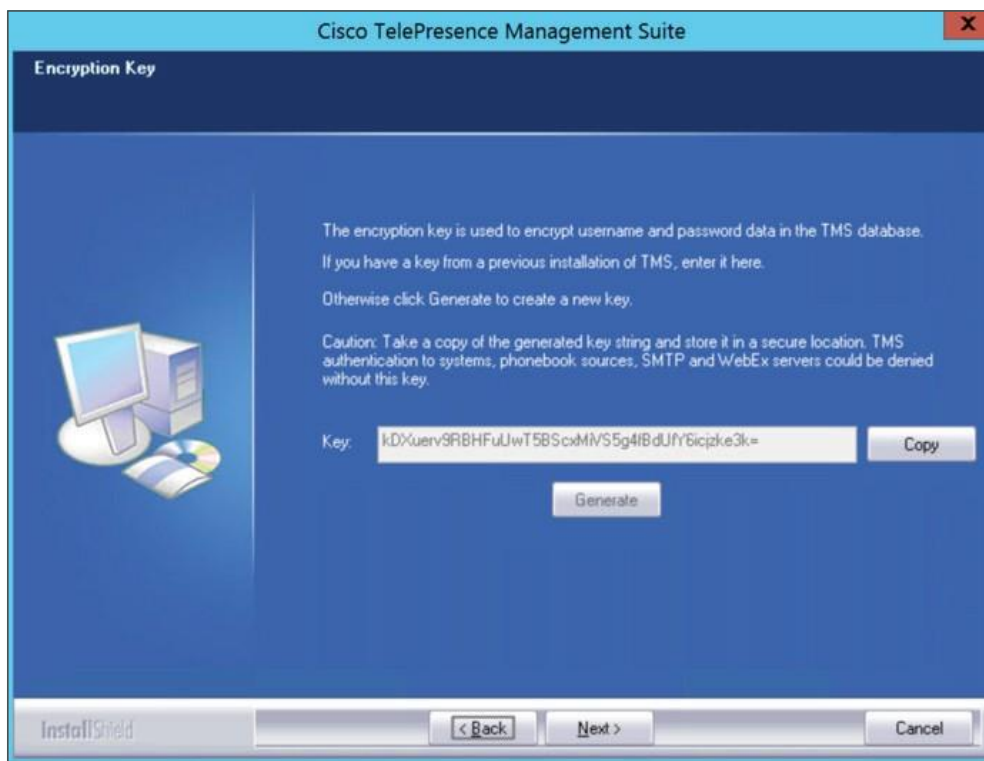
Step 11. On the **IP/ISDN Zone** page, enter the following:

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

Step 12. Click **Next**.

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

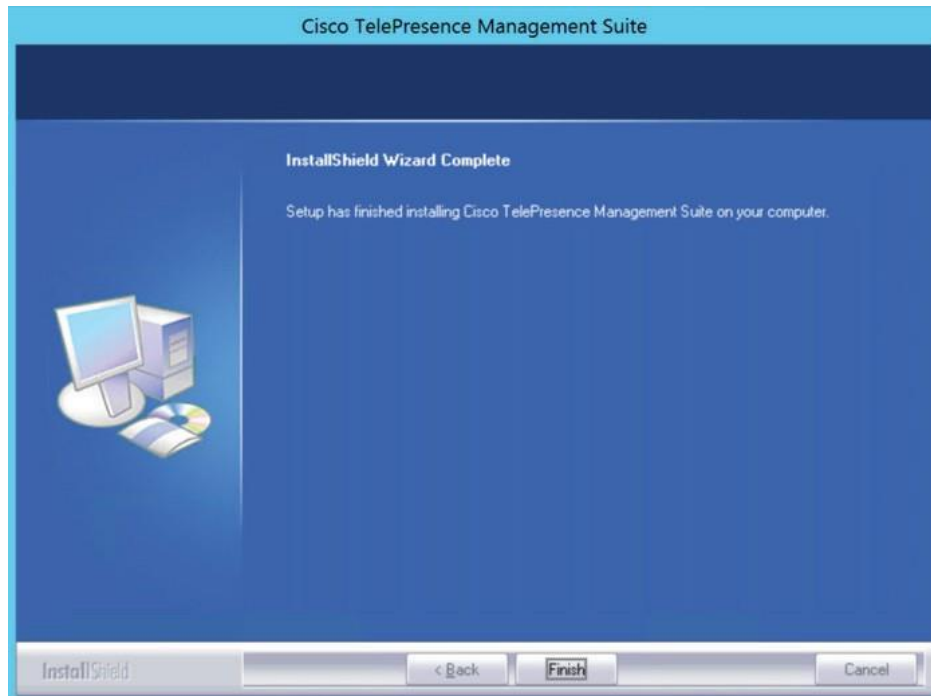
- Step 14.** On the **Encryption Key** page, click **Generate** to generate the new encryption key and click **Copy**.



- 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.



The setup wizard is complete and TMS is installed.

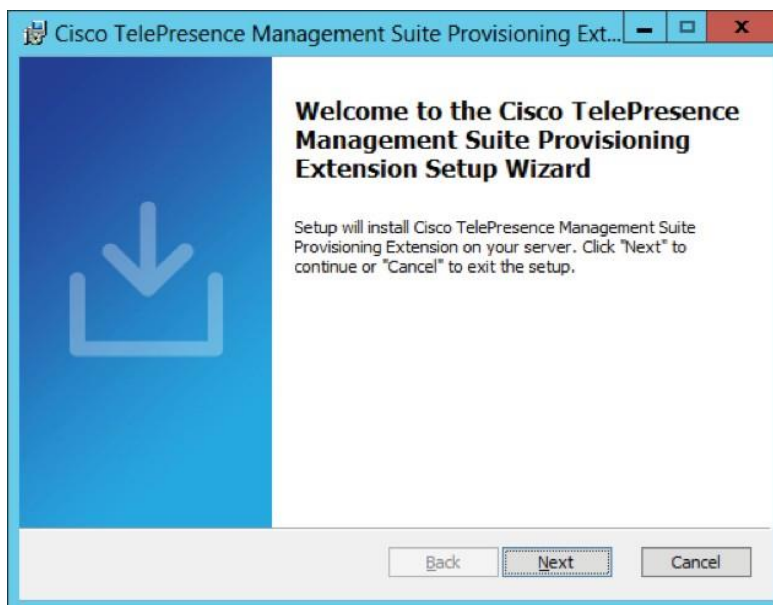
Procedure 3

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 8 is installed.
- Step 3.** Extract the TMSPE installer from the zip archive to the TMS server.

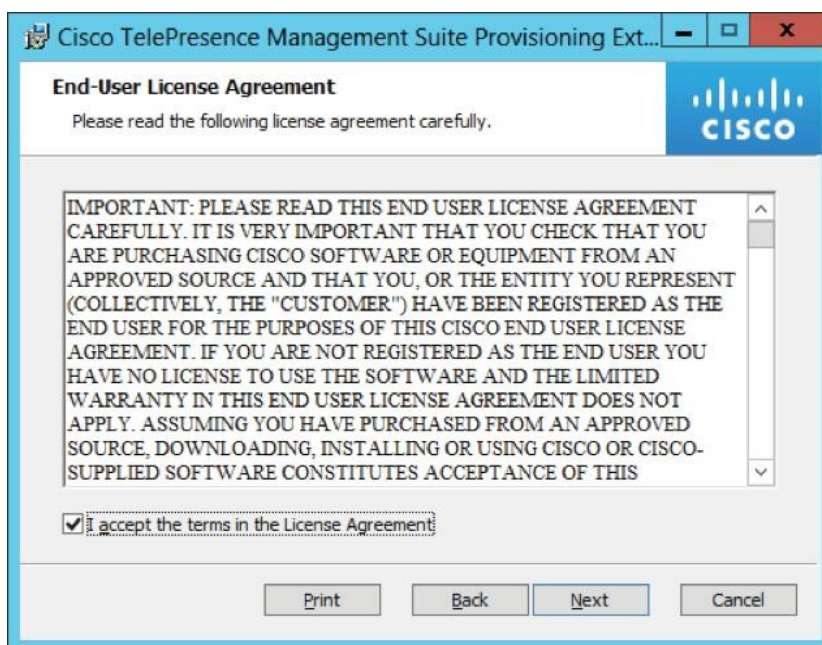


Step 4. Run the TMSPE installer as **administrator**.

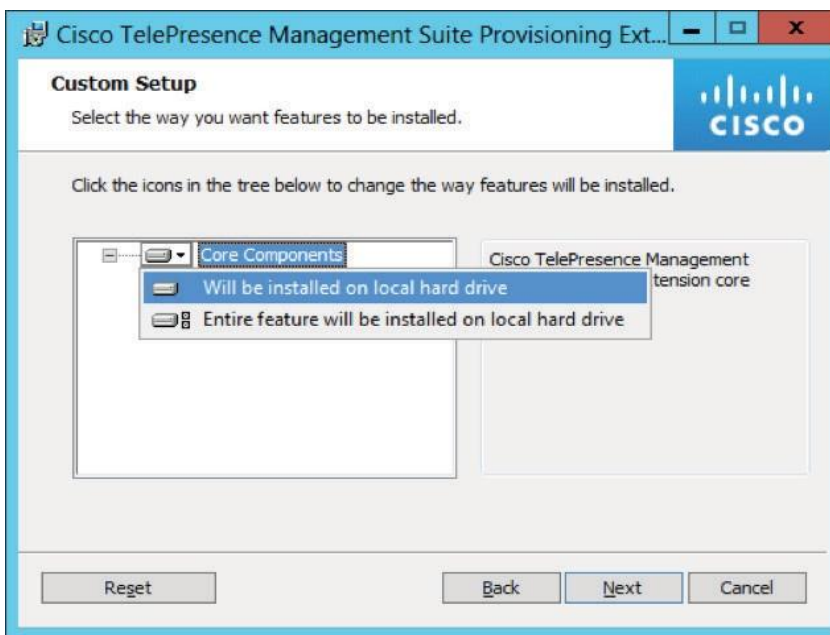


Step 5. Click **Next**.

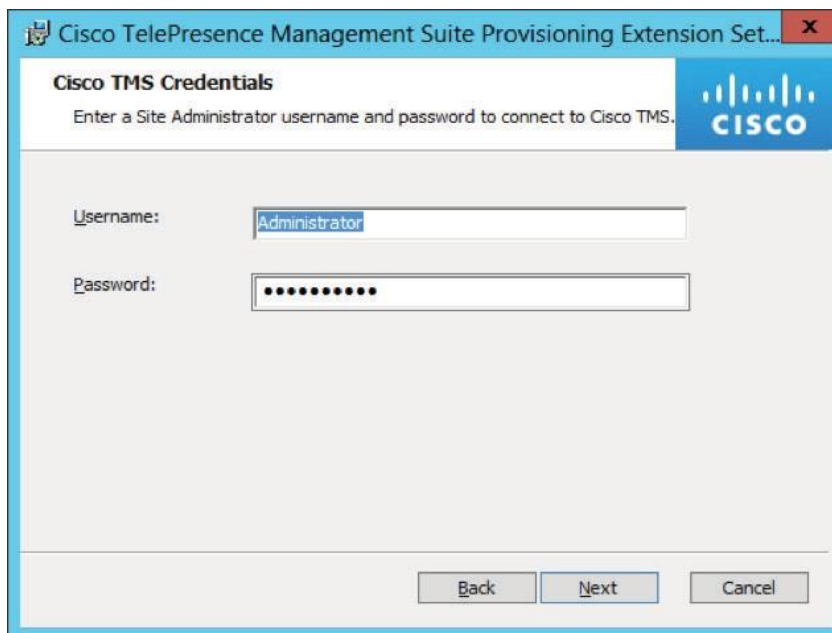
Step 6. On the **End-User License Agreement** page, select the **I agree the terms in the License Agreement** checkbox and click **Next**.



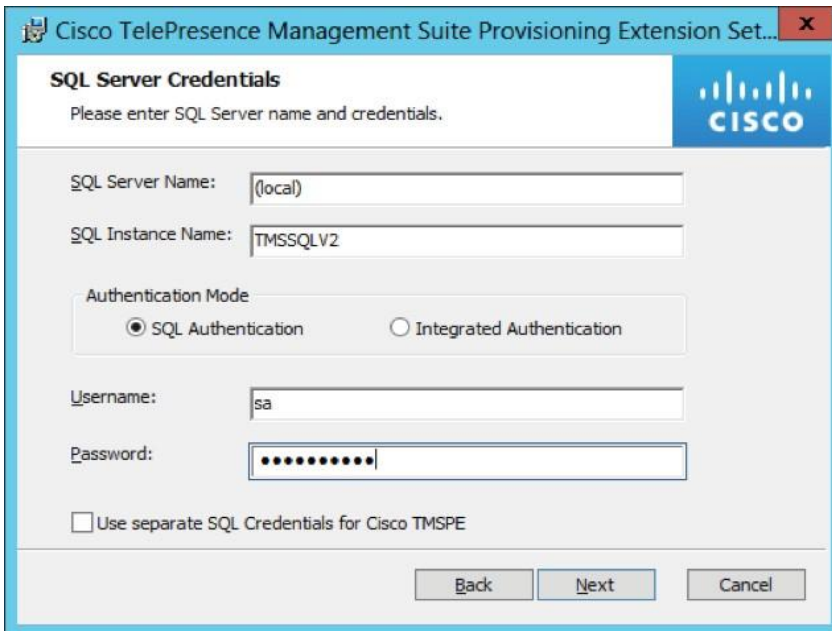
- Step 7.** On the **Custom Setup** page, click on the component icons and select the **Will be installed on local hard drive** for all the components and click **Next**.



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



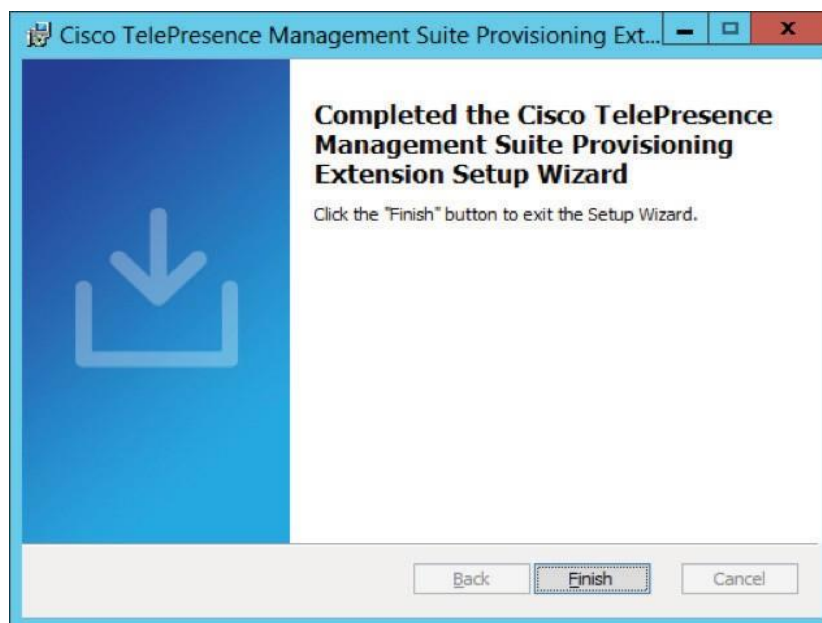
Step 9. On the **SQL Server Credentials** page, enter the SQL Server information and click **Next**.



The screenshot shows the 'SQL Server Credentials' dialog box. The title bar reads 'Cisco TelePresence Management Suite Provisioning Extension Set...'. The dialog has a Cisco logo in the top right corner. The main text says 'Please enter SQL Server name and credentials.' Below this are several input fields: 'SQL Server Name' with '(local)' entered, 'SQL Instance Name' with 'TMSSQLV2' entered, 'Authentication Mode' with 'SQL Authentication' selected (radio button), 'Username' with 'sa' entered, and 'Password' with a masked field of dots. At the bottom, there is a checkbox for 'Use separate SQL Credentials for Cisco TMSPE' which is unchecked, and three buttons: 'Back', 'Next', and 'Cancel'.

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.



The setup wizard is complete and TMSPE is installed.



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		
Element	CVD Configuration	Site-Specific Configuration
TCS Name	TCS2	
TCS IP Address	10.106.170.203	
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		
Element	CVD Configuration	Site-Specific Configuration
Recording Alias	8610002@mmcvd.ciscolabs.com	

PROCESS

1. [Deploy OVA to Host \(Recording Only\)](#)
2. [Install Windows Server 2012 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 **TCS2** 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**.

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

Procedure 2

Install Windows Server 2012 Standard R2 (Recording Only)

- Step 1.** Install Windows Server 2012 Standard R2 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 **50 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 – **10.106.170.203**
 - 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.



Content | Technology Use Case | Design Overview | Deployment Details | Product List

i Tech Tip

Depending on windows components needing to be added, you may be 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.** Navigate to **Server Manager > Roles > Add Roles**.
- Step 2.** On the **Select Server Roles** page, click the **WebServer IIS** check box. A pop-up appears for installing the dependent features. Click **Add Features** to continue, and then Click **Next**.
- Step 3.** On the **Select Features** page, select **Net framework 3.5** and **ASP.Net 4.5** as shown in the following image. Also select **Windows Server backup and Desktop Experience**. A pop-up appears for installing the dependent features. Click **Add Features** to continue, and then click **Next**.
- Step 4.** On the **Select Role Services** page, select all the features and sub features on this page under the webserver. Click **Next**.
- Step 5.** On the **Confirmation Installation Selection** page, click on 'specify an alternate source path'. Mount the **Windows Server 2012 R2 standard Edition** image to a drive. On the **Specify alternate source path** page, specify the path **<OS Mounted drive letter>:\sources\sxs**, as shown in the image. Click **OK**.
- Step 6.** On the **Confirmation Installation selection** page, click **Install**.
- Step 7.** Once the feature installation is complete, click **Close and Restart** the system.

To add the rights to the local administrator account, follow the steps.

- Step 8.** Log on to the computer as a user, who has administrative credentials.
- Step 9.** Click **Start**. Now click **Run**, type 'Control admintools', and then click **OK**.
- Step 10.** Double-click **Local Security Policy**. In the **Local Security Settings** dialog box, click **Local Policies**,
- Step 11.** Double-click **User Rights Assignment**, and then double-click **Backup Files and Directories**. In the **Backup Files and Directories Properties** dialog box, click **Add User or Group**.
- Step 12.** In the **Select User or Groups** dialog box, type the user account that is used for setup, and then click **OK** two times.



- Step 13.** Double-click **User Rights Assignment**, and then double-click **Debug Programs**. In the **Debug Programs** dialog box, click **Add User or Group**.
- Step 14.** In the **Select User or Groups** dialog box, type the user account that is used for setup, and then click **OK** two times.
- Step 15.** Double-click **User Rights Assignment**, and then double-click **Manage auditing and security log**. In the **Manage auditing and security log** dialog box, click **Add User or Group**.
- Step 16.** In the **Select User or Groups** dialog box, type the user account that is used for setup, and then click **OK** two times.

IIS is installed on the Windows server.

Procedure 4

Install SQL Server 2012 Database Server (Recording Only)

- Step 1.** Under the **Installation** tab, click **New SQL Server stand-alone installation or add features to an existing installation**.
- Step 2.** Click **I accept the license terms**, and then click **Next**.
- Step 3.** Check the **Database Engine Services** check box, and then click **Next**.
- Step 4.** In **Instance Name** field, select the **Named instance** radio button and enter the instance name as **TCS** and then click next.
- Step 5.** In the **Service Account** field, choose **Use the built-in System account** (Local system, or Network service).



Tech Tip

SQL server collation should be set to Latin1_General_CI_AS, 'Dictionary, case insensitive, 1252 character set'.

- Step 6.** In the **Authentication Mode**, select **Mixed mode**, click **Enter** and confirm the SA (system administrator) password.

SQL server is installed.

Procedure 5

Install TCS on the Windows Server (Recording Only)

- Step 1.** Log in to the windows server as a Local Administrator.



- Step 6.** In the command prompt, run the **PreInstaller.cmd** from the extracted **S_7_1_TCSBE6K_Bundle.zip** directory to configure the Content Server Pre-Installer.
- Step 7.** Run **S7_1_VM.exe** to install the VM Content Server software on the appliance. Follow the prompts to complete the TCS installation.
- Step 8.** 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

1. [Create a user for TelePresence Conductor](#)
2. [Configure SIP](#)

Procedure 1

Create a User for TelePresence Conductor

For TelePresence Conductor to communicate with the TelePresence Server, it must use credentials of 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	<input type="text" value="CondAdmin"/>
Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
Re-enter password	<input type="password" value="*****"/>
Access rights	<input type="text" value="Administrator"/>
<input type="button" value="Add user"/>	

- Step 4.** Click **Add user**.
- Step 5.** Enable HTTPS by going to **Network > Services**, enter the following value and click **Apply changes**:
 - HTTPS checked—**443**

The user is created.



Procedure 2

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 and click **Apply changes**:

- Outbound call configuration—**Call Direct**
- Outbound address—Leave Blank
- Outbound domain—Leave Blank
- Outbound Transport—**TLS**
- Advertise Dual IPv4/IPv6—**Disabled**

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

SIP is configured.



Content

Technology Use Case

Design Overview

Deployment Details

Product List

Configuring Cisco TelePresence Conductor

PROCESS

1. [Create a User for Unified CM Access \(for Ad-Hoc Conference\)](#)
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 TelePresence 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 TelePresence Conductor](#)
15. [Add Locations to Conference Bridge Pools](#)

Procedure 1

Create a User for Unified CM Access (for Ad-Hoc Conference)

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 in to the 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 and click **Save**:
 - Name—**CucmAdmin**
 - Access level—**Read-Write**
 - Password—**[Password]**

- Web access—**No**
- API access—**Yes**
- State—**Enabled**
- Your current password - **[Password]**

Administrator accounts

You are here: [Users](#) > Administrator accounts

Configuration

Name	*	<input type="text" value="CucmAdmin"/>	<small>i</small>
Access level		<input type="text" value="Read-write"/>	<small>i</small>
Password	*	<input type="password" value="....."/>	■ Very weak <small>i</small>
Confirm password	*	<input type="password" value="....."/>	<small>i</small>
Web access		<input type="text" value="No"/>	<small>i</small>
API access		<input type="text" value="Yes"/>	<small>i</small>
State		<input type="text" value="Enabled"/>	<small>i</small>

Authorize

Your current password	*	<input type="password" value="....."/>	<small>i</small>
-----------------------	---	----------------------------------------	------------------

The user is created.

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 in to the 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 and click **Save**:

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

Administrator accounts

You are here: [Users](#) > Administrator accounts

Configuration

Name	* <input type="text" value="CMRAdmin"/>	<i>i</i>
Access level	Read-write ▾	<i>i</i>
Password	* <input type="password" value="....."/>	Very weak ▾ <i>i</i>
Confirm password	* <input type="password" value="....."/>	<i>i</i>
Web access	No ▾	<i>i</i>
API access	Yes ▾	<i>i</i>
State	Enabled ▾	<i>i</i>

Authorize

Your current password	* <input type="password" value="....."/>	<i>i</i>
-----------------------	------------------------------------------	----------

The user is created.

Procedure 3

Create a User for TMS-Scheduled Conference Access

- Step 1.** Log in to the 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 and click **Save**:

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

Administrator accounts

You are here: [Users](#) ▸ Administrator accounts

Configuration

Name	*	<input type="text" value="TMSAdmin"/>		<i>i</i>
Access level		<input type="text" value="Read-write"/>		<i>i</i>
Password	*	<input type="password" value="....."/>	Very weak	<i>i</i>
Confirm password	*	<input type="password" value="....."/>		<i>i</i>
Web access		<input type="text" value="No"/>		<i>i</i>
API access		<input type="text" value="Yes"/>		<i>i</i>
State		<input type="text" value="Enabled"/>		<i>i</i>

Authorize

Your current password	*	<input type="password" value="....."/>		<i>i</i>
-----------------------	---	----------------------------------------	--	----------

The user is created.

Procedure 4

Change the System Settings

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

- System host name—**cond-1**



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

<i>i</i>	Tech Tip
The FQDN of TelePresence Conductor is cond-1.mmcvd.ciscolabs.com	

DNS

DNS settings

System host name *i*

Domain name *i*
















DNS requests port range *i*

Default DNS servers



Address 1 *i*

Step 2. Navigate to **System > Time** and set **NTP server 1** to **10.106.170.130**.

TimeYou are here: [System](#)**NTP servers**

NTP server 1	Address	<input type="text" value="10.106.170.130"/>
	 Authentication	<input type="text" value="Disabled"/>  
NTP server 2	Address	<input type="text"/>
	 Authentication	<input type="text" value="Disabled"/>  
NTP server 3	Address	<input type="text"/>
	 Authentication	<input type="text" value="Disabled"/>  
NTP server 4	Address	<input type="text"/>
	 Authentication	<input type="text" value="Disabled"/>  
NTP server 5	Address	<input type="text"/>
	 Authentication	<input type="text" value="Disabled"/>  

Time zone

Time zone	<input type="text" value="Asia/Kolkata"/>  
-----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Step 3. 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	-	✓✓✓✓✓✓✓✓

System settings are set.

Procedure 5

Add IP Addresses for Instant, Personal and Scheduled CMR Conference Locations on TelePresence 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 are added correctly.

IP You are here: [System](#) > [Network interface](#)

Configuration

IPv4 gateway * 10.106.170.129 i

LAN 1

IPv4 address * 10.106.170.139 i

IPv4 subnet mask * 255.255.255.128 i

IPv4 subnet range 10.106.170.128 - 10.106.170.255

Maximum transmission unit (MTU) * 1500 i

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 configuration](#)

Service Preference

Service Preference name * HQ Service Preference 1

Description Service Preference 1 for HQ

Conference bridge type TelePresence Server ⓘ

Pools

Priority	Pool name
	Please select ⌵

Add selected pool Delete pool Select all Unselect all

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

The service preference is created.

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	*	<input type="text" value="HQ vTS 1"/>
Description		<input type="text"/>
State		Enabled ⌵ ⓘ
IP address or FQDN	*	<input type="text" value="10.106.170.169"/>
Protocol		HTTPS ⌵ ⓘ
Port	*	<input type="text" value="443"/> ⓘ
Conference bridge username	*	<input type="text" value="CondAdmin"/>
Conference bridge password		<input type="password" value="....."/>
Dial plan prefix		<input type="text"/>
Conference bridge type	*	TelePresence Server ⌵ ⓘ
Conference bridge pool	*	HQ-Pool1 ⌵ ⓘ
SIP port	*	<input type="text" value="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
<input type="checkbox"/>	HQ vTS 1	10.106.170.169	✔ Enabled	CondAdmin		Active

The conference bridge pool is created.

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

Add selected pool Delete pool Select all Unselect all

Save Delete Cancel

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

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

Pools

Priority	Pool name	Change order	Pools to use for scheduling
<input type="checkbox"/>	1 HQ-Pool1		<input checked="" type="radio"/>

Please select

The conference bridge pool is added in the service preference.

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: C

Modify conference template

Name	* Ad-Hoc Template 1
Description	
Conference type	Meeting ⓘ
Call Policy mode	Off ⓘ
Service Preference	* HQ Service Preference 1 ⓘ Conf
Limit number of participants	<input type="checkbox"/> Maximum [] associated with this template.
Limit the conference duration (minutes)	<input type="checkbox"/> 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**.

The conference template is created.

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	<input type="checkbox"/> Maximum [] associated with this template.
Limit the conference duration (minutes)	<input type="checkbox"/> 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**.

The conference template is created.

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 <input type="button" value="i"/>
Call Policy mode	Off <input type="button" value="i"/>
Service Preference	* HQ Service Preference 1 <input type="button" value="i"/> Con
TelePresence Server	
Maximum number of cascades	* 0 <input type="button" value="i"/>
Limit number of participants	<input type="checkbox"/> Maximum <input type="text"/>
	auto-dialed participants associated with this
Limit the conference duration (minutes)	<input type="checkbox"/> Maximum <input type="text"/>
Participant quality	HD (720p 30fps video, stereo audio) <input type="button" value="i"/>
Allow multiscreen	No <input type="button" value="i"/>
Optimize resources	Yes <input type="button" value="i"/>
Content quality	1280 x 720p 5fps <input type="button" value="i"/>
Scheduled conference	Yes <input type="button" value="i"/>
Segment switching	No <input type="button" value="i"/>

Step 3. Configure other entries as required.

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



The conference template is created.

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 i
Conference template	* MeetMe Template 1 ▾
Role type	type: TelePresence Server Participant ▾ i
Allow conference to be created	Yes ▾ i

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

The conference alias is created.







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 
Role type	type: TelePresence Server Participant  
Allow conference to be created	Yes  

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

The conference alias is created.

**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 <input type="button" value="v"/> <input type="button" value="i"/>

Ad hoc conference settings	
Ad hoc IP address (local)	* 10.106.170.143 <input type="button" value="v"/> <input type="button" value="i"/>
Template	* Ad-Hoc Template 1 <input type="button" value="v"/>

Rendezvous conference settings	
Rendezvous IP address (local)	* 10.106.170.144 <input type="button" value="v"/> <input type="button" value="i"/>

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 <input type="button" value="i"/>
Trunk 2	IP address Port 5061 <input type="button" value="i"/>
Trunk 3	IP address Port 5061 <input type="button" value="i"/>
Trunk transport protocol	TLS <input type="button" value="v"/> <input type="button" value="i"/>

Step 3. Click Add location.

The location is created.

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**.

The screenshot shows the 'Conference bridge pools' configuration page. The breadcrumb trail is 'You are here: Conference configuration > Conference bridge pools'. The configuration form includes the following fields:

- 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**.

The location is added to the conference bridge pool.

i Tech Tip

For TelePresence Conductor redundancy, please refer to the latest [Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide](#).



Configuring Cisco TelePresence Management Suite (TMS)

PROCESS

1. [Enable TMSPE on TMS](#)
2. [Setup Users on TMS](#)
3. [Add TelePresence Conductor for CMR on TMS](#)
4. [Setup CMRs on TMS](#)
5. [Add TelePresence Conductor for Scheduling on TMS](#)
6. [Create Conference Alias on TMS](#)
7. [Configure Conference Settings on TMS](#)

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** and Click **Save**.

General Settings		You are
Enable Auditing:	<input type="text" value="No"/>	
Provisioning Mode:	<input type="text" value="Provisioning Extension"/>	
Enable Login Banner:	<input type="text" value="No"/>	

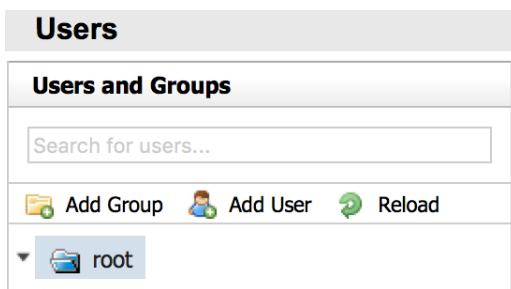
TMSPE is enabled.

Procedure 2

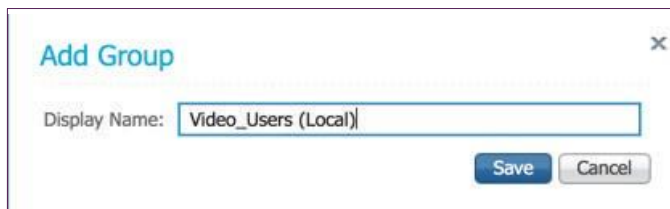
Setup Users on TMS

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

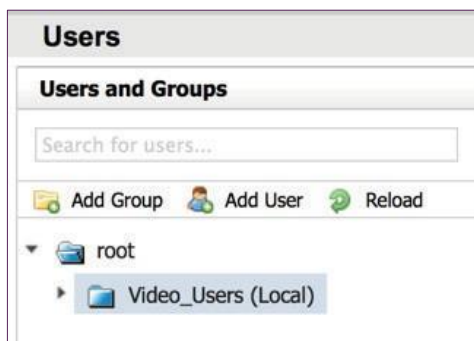
Step 2. Click on **Root** and then click on **Add Group**.



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

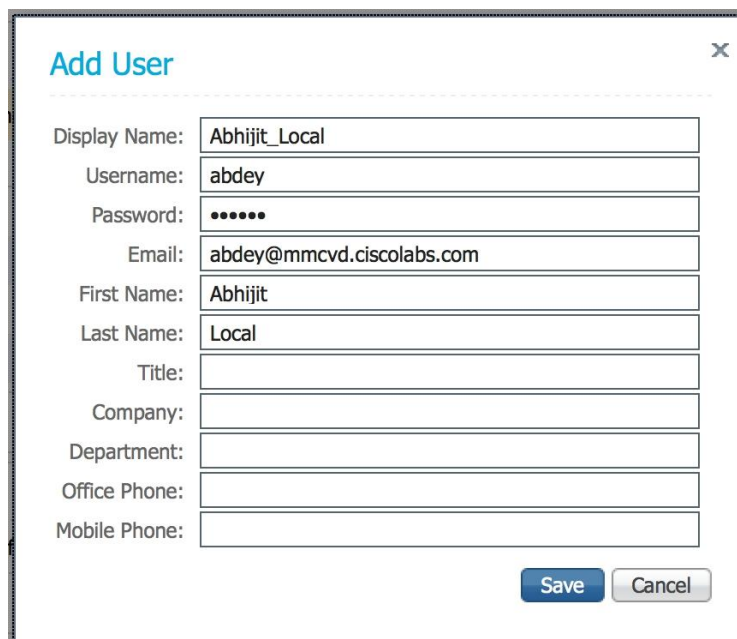


Step 4. Click on **Add User**.



Step 5. Enter the following into the relevant fields, leaving other fields at their default values and click **Save**.

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



The screenshot shows a dialog box titled "Add User" with a close button (X) in the top right corner. The dialog contains several input fields for user information. The fields and their values are as follows:

Field	Value
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:	

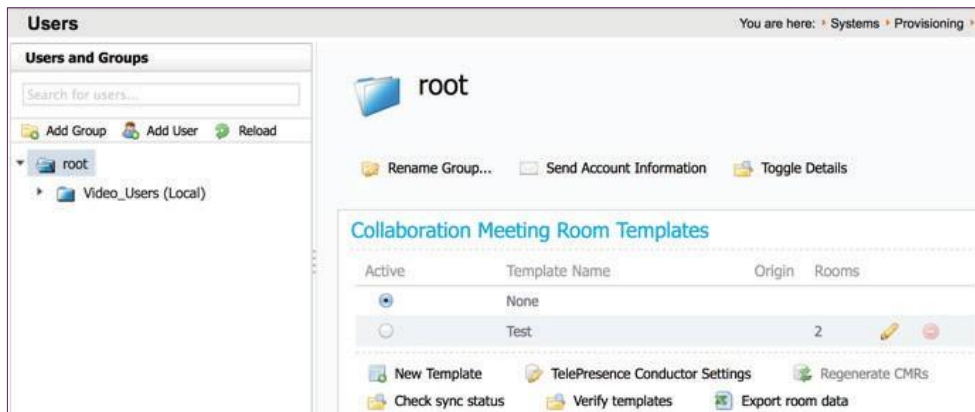
At the bottom right of the dialog, there are two buttons: "Save" (highlighted in blue) and "Cancel".

The user is created.

Procedure 3

Add TelePresence Conductor for CMR on TMS

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



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 and click **Save**.

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

TelePresence Conductor Configuration ✕

Hostname/IP:

Name:

Port:

Username:

Password:

Domain:

The TelePresence Conductor is added.



Procedure 4

Setup CMRs on TMS

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



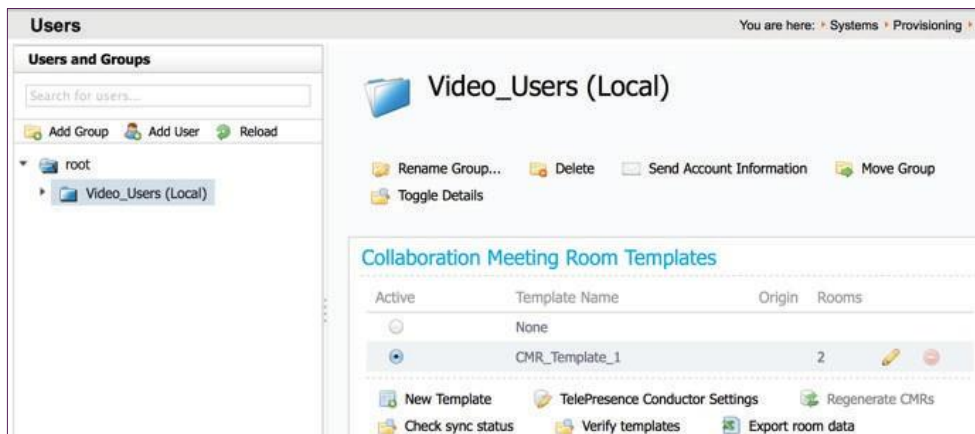
Step 2. Under Collaboration Meeting Room Templates, click New Template.

Step 3. Enter the following into the relevant fields, leaving the other fields at their default values and click **Save**.

- 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 xTemplate Name: TelePresence Conductor: Service Preference: Multiparty License Mode: SIP Alias Pattern: Numeric Alias Pattern: Type: Number Ranges: Maximum Conference Quality: Content Sharing: Maximum Content Quality: Minimum Host PIN Length: Allow Guest Role: Minimum Guest PIN Length: Guest Lobby: Limit Number of Participants:

- Step 4.** Select the radio button for **CMR_Template_1** under the **Collaboration Meeting Room Templates** and click **Yes**.

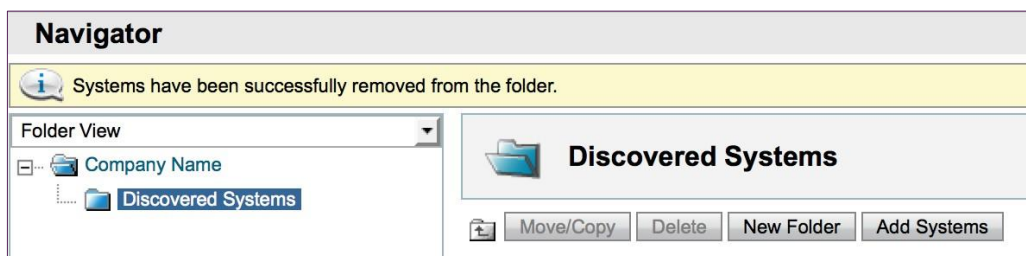


The CMR template is applied to all the users in **Video_Users (Local)** group.

Procedure 5

Add TelePresence 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.





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**

Add by Address	Add from Unified CM or TMS	Add Unmanaged Endpoint	Add Unmanaged Bridge	Pre-n
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 - 10.1.1.255				
<input type="text" value="10.106.170.139"/>				
Location Settings				
ISDN Zone:	<input type="text" value="HQ"/>	IP Zone:	<input type="text" value="HQ"/>	
Time Zone:	<input type="text" value="(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi"/>			
Advanced Settings				
Username:	<input type="text" value="TMSAdmin"/>			
Password:	<input type="text" value="*****"/>			
SNMP Community Names:	<input type="text" value="public,Public"/>			
Persistent Template:	<input type="text" value="No Template"/>			
Usage Type:	<input type="text" value="Meeting Room"/>			

Step 4. Click Next.

Step 5. Click Finish Adding Systems.

The telepresence conductor is added in TMS.



Procedure 6

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 and click **Save**.
 - 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

The conference alias is created.

Procedure 7

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**

Summary	Settings	TelePresence Conductor	Conference Bridges	Connection
View Settings	Edit Settings	Extended Settings	Ticket Filters	
Extended Settings				
Numeric ID Base:	<input type="text" value="1000"/>			
Numeric ID Step:	<input type="text" value="1"/>			
Numeric ID Quantity:	<input type="text" value="Unlimited"/>			
Conference Layout:	<input type="text" value="Default View Family"/>			
Limit Ports to Number of Scheduled Participants:	<input type="text" value="On"/>			
<input type="button" value="Save"/>				

- 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**. And click **Save**.

Advanced	
External MCU Usage in Routing:	<input type="text" value="Only if needed"/>
Preferred MCU Type in Routing:	<input type="text" value="Cisco TelePresence Conductor"/>

The conference settings are configured.



Configuring Cisco Unified Communications Manager (Unified CM)

Easy Access Configuration Sheet

Cisco Unified CM Configuration Requirements		
Element	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 TelePresence 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 TelePresence Conductor as Conference Bridge](#)
11. [Configure MRG and MRGL for Video and Add TelePresence 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**.

The screenshot shows the 'Region Configuration' page with a 'Save' button at the top. Below it is the 'Region Information' section, where the 'Name*' field is populated with 'Video_Reg'.

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

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

The screenshot shows the 'Modify Relationship to other Regions' page. It has four columns: 'Regions', 'Audio Codec Preference List', 'Maximum Audio BR Rate', and 'Maximum Session Bit Rate for Video Calls'. In the 'Regions' column, 'Default' is selected. In the 'Maximum Session Bit Rate for Video Calls' column, the value '32256 kbps' is entered and selected.

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

The region is configured.

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 and click **Save**.

- 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

The device pool is configured.



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 Conferencing [View Details](#)

DTMF Signaling Method* No Preference

Normalization Script

Normalization Script cisco-telepresence-conductor-interop

Step 5. Click **Save**, and then click **Reset**.

Step 6. Now click **Reset** again on the pop-up window that opens up and click **close**.

The Unified CM trunk is configured to the TelePresence Conductor for personal and scheduled CMR conferences.

Procedure 4

Configure Unified CM Trunk to TelePresence 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 Conferencing [View Details](#)
 DTMF Signaling Method*: No Preference

Normalization Script

Normalization Script: cisco-telepresence-conductor-interop

Step 5. Click **Save**, and then click **Reset**.

Step 6. Now click **Reset** again on the pop-up window that opens up and then click **Close**.

The trunk is configured.

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 and click **Save**.

- 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*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

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*

The SIP trunk security profile is configured.




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 and click **Save**.

- 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*

Early Offer support for voice and video calls*

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

The sip profile is configured.

Procedure 7

Configure Unified CM Trunk to Cisco TCS (for Recording only)

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-TCS2**
- Device Pool—**Video_DP**
- Destination Address—**10.106.170.203**
- Destination Port—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile**
- SIP Profile—**SIP Profile for Cisco TCS**

Device Information	
Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TR1-TCS2
Description	
Device Pool*	Video_DP

SIP Information			
Destination			
<input type="checkbox"/> Destination Address is an SRV			
	Destination Address	Destination Address IPv6	Destination Port
1 *	10.106.170.203		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*	SIP profile for Cisco TCS View Details		

Step 5. Click Save.



Step 6. Click **Reset**.

Step 7. Click **Reset** on the pop-up window that opens up.

Step 8. Click **Close**.

The trunk is configured.

Procedure 8

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 and click **Save**.

- 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
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace	< None >
Network Domain	
Route Class*	Default
Gateway/Route List*	TR1-Cond1-static-10.106.170.143
Route Option	<input checked="" type="radio"/> Route this pattern

The route pattern is configured.



Content

Technology Use Case

Design Overview

Deployment Details

Product List

Procedure 9

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** to create a new route pattern.
- Step 2.** Enter the following in the relevant fields, leaving other fields at their default values and click **Save**.
- Route Pattern—**861XXXX**
 - Gateway/Route List—**TR1-TCS2**

Pattern Definition	
Route Pattern*	861XXXX
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority	< None >
Namespace Network Domain	
Route Class*	Default
Gateway/Route List*	TR1-TCS2

The route pattern is configured.

Procedure 10

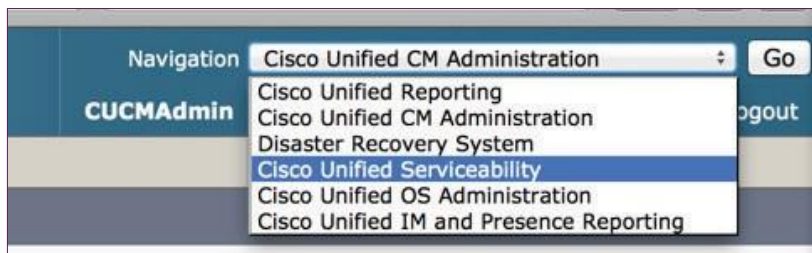
Configure Unified CM SIP Route Pattern for Personal CMR Conferences

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. mmcvd.ciscolabs.com) 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.

The following steps will configure the Unified CM to enable ILS and import the perpersonal CMR conference URLs.

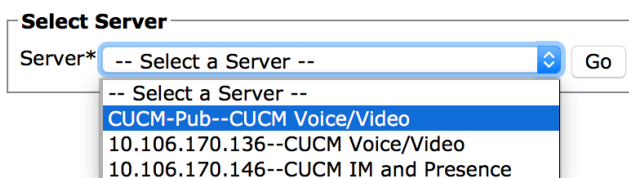
- Step 1.** Click the **Navigation** tab on the top right corner of the **Unified CM Administration** page, select **Cisco Unified Serviceability** from the dropdown list and click **Go**.



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



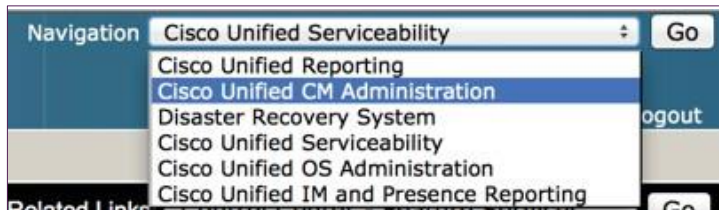
- Step 3.** Select **CUCM-Pub--CUCM Voice/Video** from the drop-down list under the **Server** field, and click **Go**.



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

Database and Admin Services	
	Service Name
<input checked="" type="checkbox"/>	Cisco Bulk Provisioning Service
<input checked="" type="checkbox"/>	Cisco AXL Web Service
<input checked="" type="checkbox"/>	Cisco UXL Web Service
<input checked="" type="checkbox"/>	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. Select the **Cisco Unified CM Administration**, and then click **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**, select **Hub Cluster** as the **Role** under the **Intercluster Lookup Service Configuration** tab, and then click **Save**.

Intercluster Lookup Service Configuration

Role

- 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_CMV_DP_Catalog**
- Route String—**cmr.mmcvd.ciscolabs.com**

Imported Global Dial Plan Catalog Information

Name*

Description

Route String*

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: * cvd_cmr.csv

Select The Target *

Select Transaction Type *


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_CMV_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_CMV_DP_Catalog
Job Information	
Job Description	Insert Imported Directory URIs and Patterns
<input checked="" type="radio"/> Run Immediately	<input type="radio"/> Run Later (To schedule and activate this job, use Job Schedu
<input type="button" value="Submit"/>	

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 and click **Save**.

- 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

The SIP route pattern is configured.

Procedure 11

Configure TelePresence Conductor as Conference Bridge

This procedure describes configuring TelePresence 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*

Description

Conference Bridge Prefix

SIP Trunk*

Allow Conference Bridge Control of the Call Security Icon

HTTP Interface Info

Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1

Username*

Password*

Confirm Password*

Use HTTPS

HTTP Port*

Step 3. Click Save.

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

<input type="checkbox"/> MR-cond-1	Registered with CUCM-Pub	10.106.170.144
----------------------------------------------------	-----------------------------	----------------




Content | Technology Use Case | Design Overview | **Deployment Details** | Product List

- Step 5.** Navigate to **Media Resources > Media Resource Group**, and then click **Add New**.
- Step 6.** In **Name**, enter **MRG-1-cond-1**.
- Step 7.** In **Available Media Resources**, select **MR-cond-1 (CFB)** and click the down arrow to move it down to the **Selected Media Resources**.
- Step 8.** 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 9.** Navigate to **Media Resources > Media Resource Group List**, and then click **Add New**.
- Step 10.** In **Name**, enter **MRGL-1-cond-1**

Step 11. 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 and click **Save**.

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

The telepresence conductor is configured as a media resource.

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** and click **Save**.

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

The MRGL is added.

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 and click **Save**.

- SIP enabled - **checked**
- SIP display name - **TCS2**
- Registration - **Trunk**
- Server Address - **10.106.170.135**
- Transport - **TCP**

SIP enabled	<input checked="" type="checkbox"/>
SIP display name	TCS2
SIP address (URI)	
Server discovery	Manual
Registration	<input type="radio"/> Terminal <input checked="" type="radio"/> Trunk
Trunk Peer Polling Interval	10
Server address	10.106.170.135
Server type	Auto
Transport	TCP

The site settings are configured.

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 and click **Save**.

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



Recording alias	
Name	Recording Alias 1 (Admin) *
Recording alias type	<input checked="" type="radio"/> Personal ⓘ <input type="radio"/> 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) ⓘ

The recording alias is configured.



Content

Technology Use Case

Design Overview

Deployment Details

Product List

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*

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**

Phone Type

Product Type: Cisco TelePresence EX60
Device Protocol: SIP

Device Information

Device is trusted

MAC Address*

Description

Device Pool*

Common Device Configuration

Phone Button Template*

Step 5. Click **Save**.

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



Association

Modify Button Items

1 7718 Line [1] - Add a new DN 7719

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

Directory Number Information

Directory Number*

Route Partition

Description

Alerting Name

ASCII Alerting Name

External Call Control Profile

Allow Control of Device from CTI

Associated Devices

Step 8. Under Directory URIs, enter **8001001@mmcvd.ciscolabs.com** as the URI and click **Add Row**.

Directory URIs

Primary	URI	Partition
<input checked="" type="radio"/>	<input type="text" value="8001001@mmcvd.ciscolabs.com"/>	<input type="text" value=" < None >"/>

The endpoint is added.

**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**.



The endpoint is added.

Recording Self Video

PROCESS

1. [Dial TCS URI \(Recording Only\)](#)

Procedure 1

Dial TCS URI (Recording Only)

Dial **8610002@mmcvd.ciscolabs.com** and wait till the countdown finishes and is 0. Now the call to the TCS is recorded 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, click **Go and login as user**.
- Step 2.** Click on **Open Collaboration Meeting Room**.



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



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

A screenshot of the Cisco Collaboration Meeting Room (CMR) configuration interface. The top header is blue and contains the Cisco logo on the left, the text 'Collaboration Meeting Room' in the center, and the user name 'Abhijit_Local' with a menu icon on the right. The main content area has a light gray background and is titled 'Name Your CMR'. Below the title, there is a paragraph of text: '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.' Below this text is a label 'Enter CMR name (optional):' followed by a text input field containing the text 'abdey'. At the bottom of the form, there are two buttons: a gray 'Back' button and a green 'Next' button.



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

Collaboration Meeting Room Abhijit_Local

Set your CMR PIN

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

Enter PIN (optional):

[Back](#) [Finish](#)

abdey [Edit Name](#)

Details

Connect to your CMR
Video Address: abdey.cmr@mmcvd.ciscolabs.com
Call-in Number: 8510744

Create an email message containing your CMR details. [Create Email Message](#)

Your CMR meetings can include up to 4 participants.

Security

Your CMR is protected with one PIN for hosts and one PIN for guests. [Edit PIN](#)

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, click **Go** and login as user.

- 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.

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**.

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**.

Participants	Connection Settings
<input type="checkbox"/>	Main Participant
<input type="checkbox"/>	cond-1 (8211000)
<input type="checkbox"/>	cond-1 (8211000)
<input type="checkbox"/>	cond-1 (8211000)
<input type="checkbox"/>	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.

[Content](#)[Technology Use Case](#)[Design Overview](#)[Deployment Details](#)[Product List](#)

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 is recorded 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=	11.5(1)
Video Phones	Unified IP Phones 8800 series	CP-88xx-K9=	11.5(1)
	Unified IP Phones DX650	CP-DX650-K9	10.2.5
Video Endpoints	Cisco TelePresence DX70	CP-DX70-W-K9=	CE 8.2
	Cisco TelePresence DX80	CP-DX80-K9=	CE 8.2
	Cisco TelePresence SX10	CTS-SX10N-K9	CE 8.2
	Cisco TelePresence SX20	CTS-SX20N-PHD2.5X-K9	CE 8.2
Conference Bridge Controller	Mid Market Virtual TelePresence Conductor	R-VMCNDTRM-K9	4.2
	Cisco TelePresence Management Suite	CTI-TMS-SW-K9	15.2
	Cisco TelePresence Management Suite Provisioning Extension		1.7
Video Conference Bridge	Virtual TelePresence Server	R-VTS-K9	4.3
Video Recording Server	Cisco TelePresence Content Server	BE6K-VMTCS-1R-1L	7.1
Soft Client	Cisco Jabber for Windows	JAB9-DSK-K9	11.6



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)