Video Conferencing Using Cisco BE 6000

TECHNOLOGY DESIGN GUIDE

February 2014

Table of Contents

Preface

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

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

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

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd/collaboration

CVD Navigator

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

Use Cases

This guide addresses the following technology use cases:

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

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

Scope

This guide covers the following areas of technology and products:

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

For more information, see the “Design Overview” section in this guide

Proficiency

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

- CCNA Video—1 to 3 years configuring voice devices and video single-screen endpoints, supporting telephony and video applications, and troubleshooting.
- CCNA Voice—1 to 3 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Related CVD Guides

Cisco Preferred Architecture for Collaboration

Unified Communications Using Cisco BE 6000 Technology Design Guide

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

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. The time away from home and the frustration levels experienced from lost luggage, navigating through airport terminals, and driving in unfamiliar cities are burdens many employees must endure weekly.

Organizations are under increasing pressure to reduce the amount of time it takes to make informed decisions concerning their business operations. 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. Human resource departments find it is difficult and expensive to interview candidates for a position if the prospective employee is not in the same city as the hiring manager.

Technology Use Case

Audio conferences can help in certain situations, but 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. 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 design guide enables the following capabilities:

- Implement single cluster centralized design to simplify deployment and management while saving on infrastructure components.
- Use URI and numeric dialing to allow video-enabled IP phones to call room systems.
- Provisions the videoconference bridge for the site.
- Enables conference resource optimization and management.
- Enables ad-hoc and rendezvous conferencing.

Design Overview

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

Network Considerations

Cisco recommends running your video collaboration traffic over an IP network rather than a public ISDN network. 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, you will realize significant quality improvements and cost savings.

Running video over a converged IP network allows unified communications to become a reality. 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.

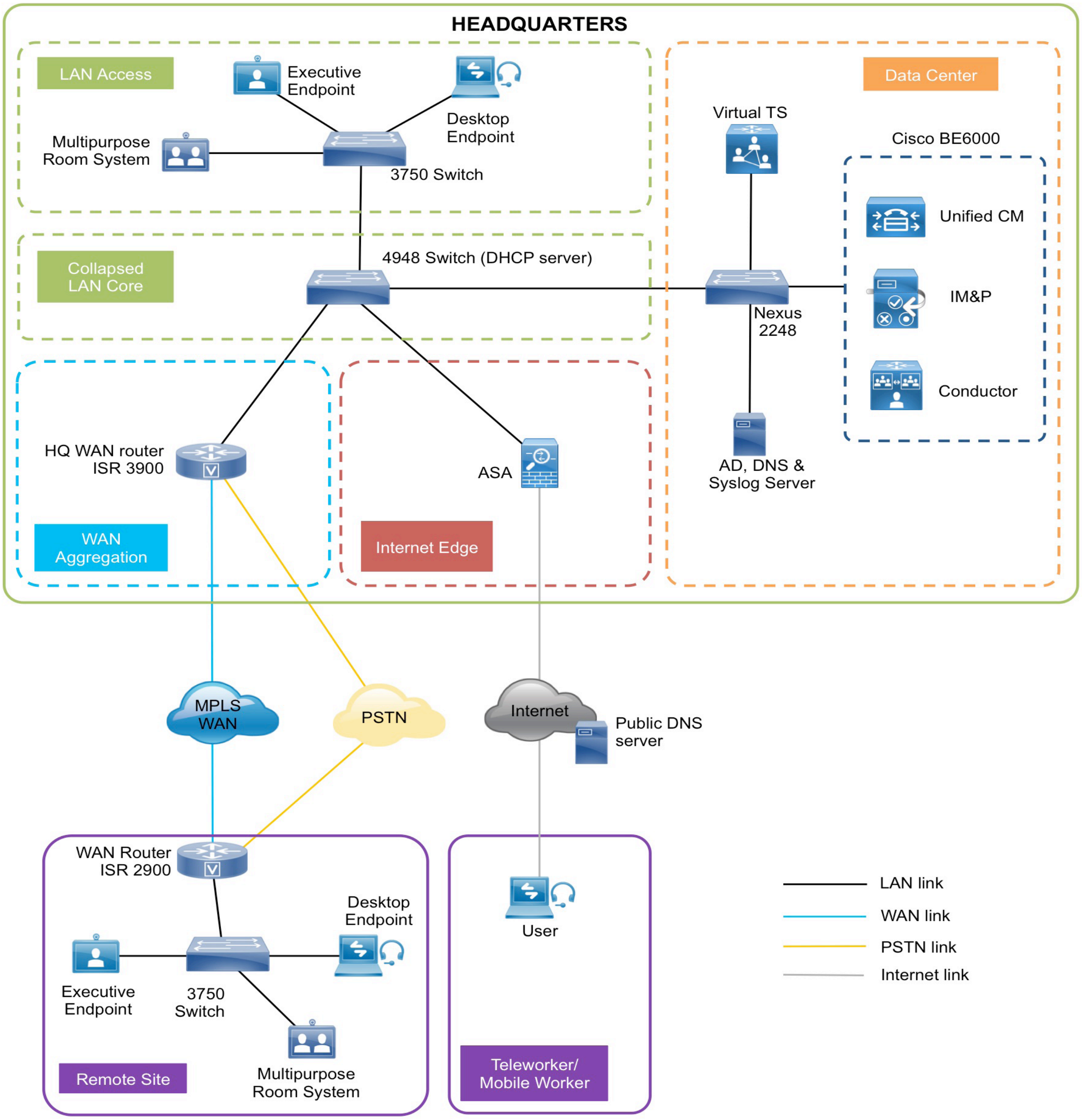
With an IP network, the ongoing costs of running video calls are minimal because you only have to pay for maintenance and technical support. When return on investment (ROI) for the initial deployment is met, any additional calls are essentially free. Because there is no incremental cost involved, employees 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 (CUCM) for call control and SIP endpoint registrations
- Desktop (Cisco Jabber, Cisco Unified IP 9900 Series IP phones, Cisco Desktop Collaboration Experience DX650 and Cisco TelePresence System EX series) and multipurpose (Cisco TelePresence SX20 Quick Set) systems for placing and receiving calls
- Cisco TelePresence Server on virtual machine and Cisco TelePresence Conductor for reservation-less, ad-hoc, and rendezvous conferences
- Network Time Protocol (NTP) server for logging consistency

Figure 1 - High level block diagram



Cisco Unified Communications Manager

CUCM (formerly *Cisco Unified CallManager*) serves as the software-based, call-processing component of Cisco Unified Communications. The CUCM system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified Communications Manager open-telephony application program interface (API).

CUCM is the primary call agent in this CVD. CUCM supports session initiation protocol (SIP), and the configurations in this document use SIP as signaling protocol for the 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 point to multi-point 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 Video endpoints–Cisco Jabber software-based desktop clients, such as Cisco Jabber for Windows, Cisco Unified IP 9900 Series Phones and the Cisco Desktop Collaboration Experience DX600 Series endpoints are capable of transmitting video by means of the built-in front-facing camera or USB attached external camera. The Cisco TelePresence System EX Series video endpoints take the personal desktop solution to a next level of experience with support for full high definition (HD) video calls and added features such as content sharing. EX Series models include the Cisco TelePresence System EX60 and EX90. The EX90 has a wider screen with support for the multisite feature that provides the ability to add participants into a Cisco TelePresence call and dual display for content sharing.
- Multipurpose endpoints–The Cisco TelePresence SX20 Quick Sets are flexible integrators that can turn any flat-panel 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 the mobile or desktop user and the immersive room-meeting participant. Compatible with a range of hardware platforms, the Cisco TelePresence Server is a versatile, highly scalable solution for mid market and larger enterprise customers. Cisco 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.

Reservation-less, ad hoc, and rendezvous conferencing use Cisco TelePresence Server on Virtual Machine (vTS) 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. Cisco 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 optimum resource usage. Conductor is mandatory when vTS is being used for conferencing.

Dial Plan

This 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@cisco.local**

The domain used in this document is **cisco.local**

For ad-hoc conferencing conductor is added as a media resource on the CUCM. For rendezvous conferencing, conductor is SIP trunked to CUCM. In this document, for the rendezvous conference bridge numbers, every user has a dedicated number configured on the conductor. The bridge numbers used to dial in and join the conferences are in the following pattern:

- **850xxxx**

Deployment Details

This guide is divided into multiple sections: server installations and deploying conferencing. Every section has procedures and steps needed to configure the system grounds up.

For the installation of Cisco Unified Communications Manager (CUCM), refer the "Installing the Cisco Unified CM" process in the Unified Communications using Cisco BE 6000 Technology Design Guide.

PROCESS

Installing Cisco TelePresence Server on Virtual Machine (vTS)

1. Configure vTS connectivity to LAN
2. Deploy OVA to host
3. Configure the VM guest
4. Apply licenses on Virtual TelePresence Server

This process guides you through installing the VM and assumes that you are using vSphere.

Procedure 1 Configure vTS connectivity to LAN

The vTS can be connected to a nexus switch in the data center.

Step 1: Using the user account that has the ability to make configuration changes, log in to the Cisco Nexus switch.

Step 2: If there is a previous configuration on the switch port where the vTS is connected, remove the individual commands by issuing a **no** in front of each command in order to bring the port back to its default state.

Step 3: Configure the port as an access port.

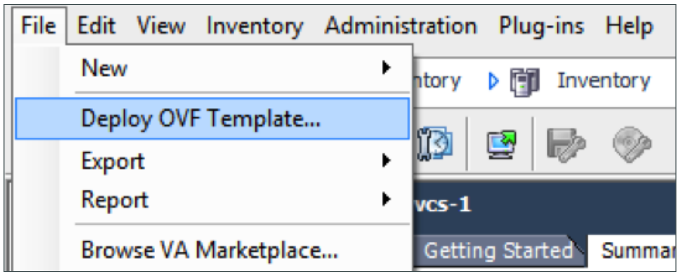
```
interface GigabitEthernet1/14
 description VCS
 switchport access vlan 20
 switchport host
```

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.

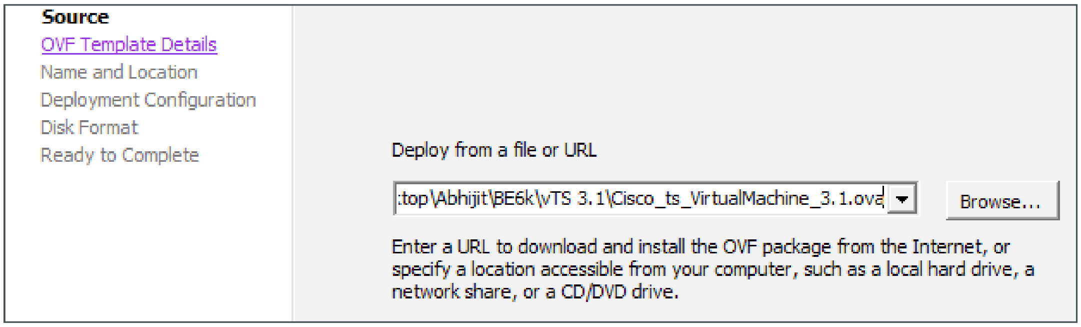
Step 1: Log in to vSphere in order to access the ESXi Host.

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



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

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



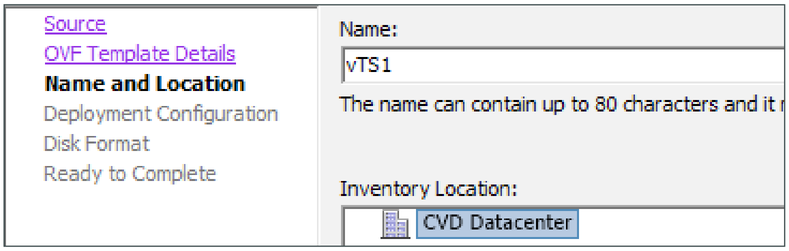
Deploy from a file or URL

:top\Abhijit\BE6k\vTS 3.1\Cisco_ts_VirtualMachine_3.1.ova

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

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

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



Name:

vTS1

The name can contain up to 80 characters and it r

Inventory Location:

CVD Datacenter

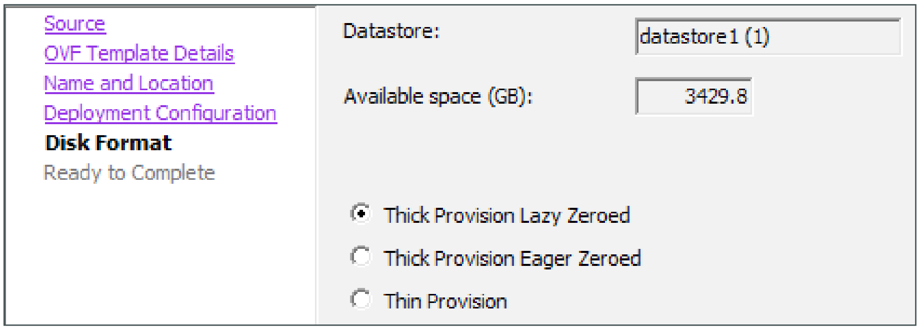
Step 7: On the Deployment Configuration page, select **Cisco_ts_VirtualMachine Hyperthread XX Core OVA** and then click **Next**.

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

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

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

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



Source
OVF Template Details
Name and Location
Deployment Configuration
Disk Format
Ready to Complete

Datastore: datastore1 (1)

Available space (GB): 3429.8

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

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 Settings.

Step 14: Select **Power on after deployment**.

Step 15: Click **Finish**.

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

Procedure 3 Configure the VM guest

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

Step 2: Create its second hard-disk partition, and then reboot. The console of the Cisco TelePresence Server VM appears.

When the TS: prompt appears, the TelePresence Server on virtual machine is ready for initial configuration.

Step 3: Configure a static IP address following the format shown in the console and press **Enter**.

```
static 192.168.1.23 255.255.255.0 192.168.1.1
```

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

Step 4: Use your browser to navigate to the IP address or host name of the device.

Tech Tip

The Cisco TelePresence Server on Virtual Machine application must operate in remotely managed mode. It must be managed through the Cisco TelePresence Conductor XC2.2 (or later), or a similar system, or through the TelePresence Server API. For more information about the TelePresence Server API, refer to the Cisco TelePresence Server API Reference Guide.

Step 5: Click **Log in** and enter the user name **admin** with no password. The Login information page appears.

Tech Tip

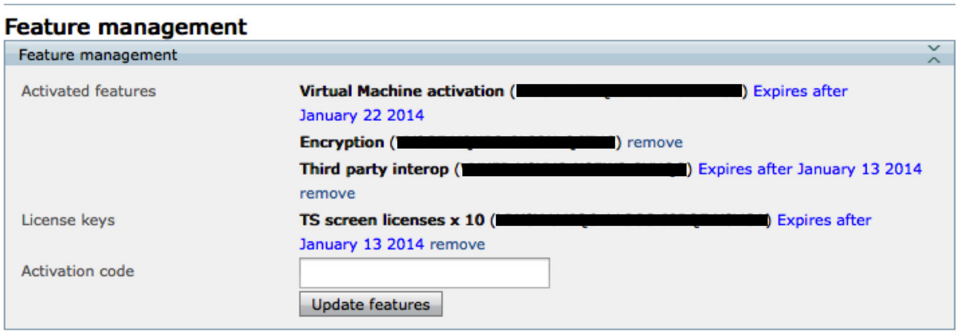
Cisco recommends that you change the admin account to use a password as soon as possible. To do that, on the Login information page, click **Change Password**.

Procedure 4 Apply licenses on Virtual TelePresence Server

Contact Cisco to get license keys for the features you have purchased.

Step 1: Go to **Configuration > Upgrade**.

Step 2: In the Feature Management section, in the Activation Code field enter the activation code for a feature license, and then click **Update features**. The feature name and license key appear under License keys.



Feature management

Feature management

Activated features	**Virtual Machine activation** ([redacted]) Expires after January 22 2014 **Encryption** ([redacted]) remove **Third party interop** ([redacted]) Expires after January 13 2014 remove
License keys	**TS screen licenses x 10** ([redacted]) Expires after January 13 2014 remove
Activation code	

Step 3: Repeat step 2 for each additional feature license.

PROCESS

Installing Cisco TelePresence Conductor

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

This process guides you through installing the VM and assumes that you are using vSphere.

Procedure 1 Configure Conductor connectivity to LAN

Conductor can be connected to a Cisco Nexus switch in the data center.

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

Step 2: If there is a previous configuration on the switch port where the Conductor is connected, remove the individual commands by issuing a **no** in front of each command in order to bring the port back to its default state.

Step 3: Configure the port as an access port.

```
interface GigabitEthernet1/20
 description VCS
 switchport access vlan 20
 switchport host
```

Procedure 2 Deploy OVA to host

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

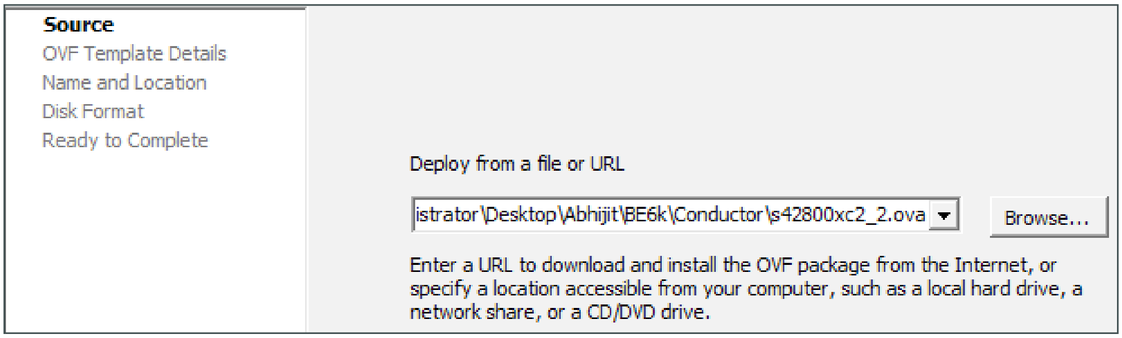
Step 2: Select **File > Deploy OVF Template**.

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

Step 4: Click **Next**.

Tech Tip

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



Deploy from a file or URL

istrator\Desktop\Abhijit\BE6k\Conductor\s42800xc2_2.ova

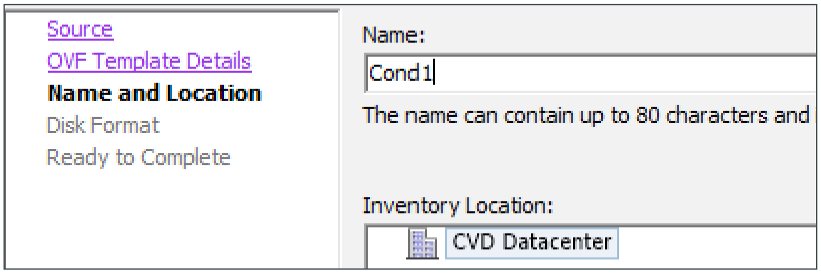
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Step 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 a **Name** for this TelePresence Conductor VM guest (for example: **Cond1**).



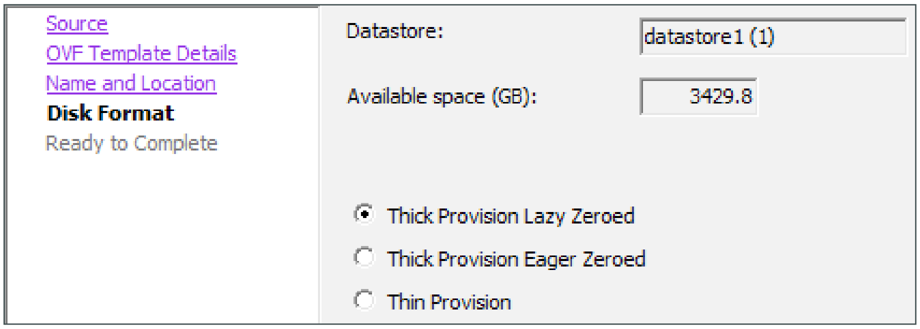
Name: Cond1

The name can contain up to 80 characters and

Inventory Location: CVD Datacenter

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**.



Datastore: datastore1 (1)

Available space (GB): 3429.8

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Tech Tip

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

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

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

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

Step 14: Click **Finish**.

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

Procedure 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.

Step 2: Create its second hard disk partition, and then reboot to a login prompt.

Step 3: At the login prompt, enter the username **admin**, and the password **TANDBERG**.

Step 4: At the Install Wizard prompt, type **y**, and then press **Enter**.

Step 5: 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: **192.168.1.20**
- Subnet Mask LAN1: **255.255.255.0**
- Default Gateway Address: **192.168.1.1**
- Ethernet Speed: **auto**
- Run ssh daemon: **y**

The configuration is applied and TelePresence Conductor logs you out.

Step 6: Log into TelePresence Conductor as root and then restart the VM guest by typing **restart**.

Step 7: You should now be able to access TelePresence Conductor via a web browser.

Procedure 4 Apply licenses on Cisco TelePresence Conductor

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

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

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

Step 4: For each option key provided, in the **Add option key** field, enter the option key value and then click **Add option**.

PROCESS

Configuring Virtual TelePresence Server (vTS)

1. Create a user
2. Configure SIP

Procedure 1 Create a user

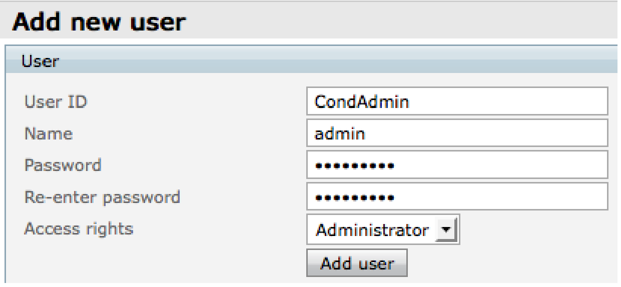
For TelePresence Conductor to communicate with the TelePresence Server, it must use credentials for a user account that has administrator rights. We recommend that you create a dedicated administrator-level user for this task.

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

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

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

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



Add new user

User

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

Step 4: Enable **HTTPS**.

Go to **Network** > **Services** and enter the following value:

- HTTPS checked—**443**

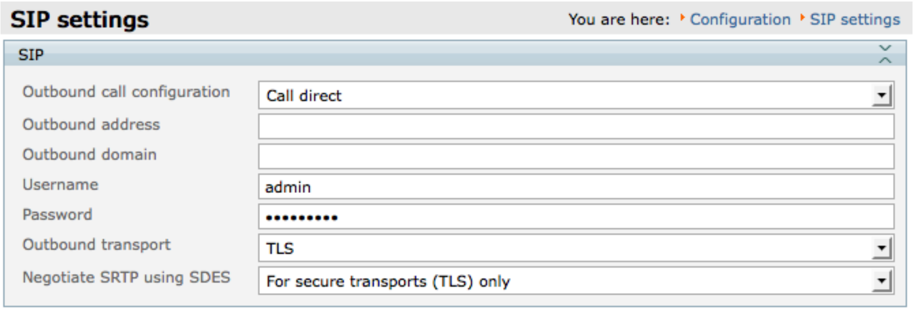
Procedure 2 Configure SIP

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:

- Outbound call configuration—**Call Direct**
- Outbound address—Leave Blank
- Outbound domain—Leave Blank
- Username—**[username]**
- Password—**[password**
- Outbound Transport—**TLS**
- Negotiate SRTP using SDES—**For Secure Transport (TLS) only**
- Use local certificate for outgoing connections and registrations—Selected



SIP settings

You are here: Configuration SIP settings

SIP

Outbound call configuration	Call direct
Outbound address	
Outbound domain	
Username	admin
Password	•••••••••
Outbound transport	TLS
Negotiate SRTP using SDES	For secure transports (TLS) only

Step 3: Click **Apply changes**.

PROCESS

Configuring Cisco TelePresence Conductor

1. Create a user for CUCM access
2. Change the system settings
3. Add IP addresses for ad-hoc and rendezvous locations on Conductor
4. Set up conference bridge pools
5. Create Service preferences
6. Create a template for an ad hoc meeting-type conference
7. Create a conference template for a rendezvous meeting-type conference
8. Create a conference alias for an ad-hoc conference
9. Create a conference alias for a rendezvous conference
10. Create locations in Conductor
11. Add locations to conference bridge pools

Procedure 1 Create a user for CUCM access

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

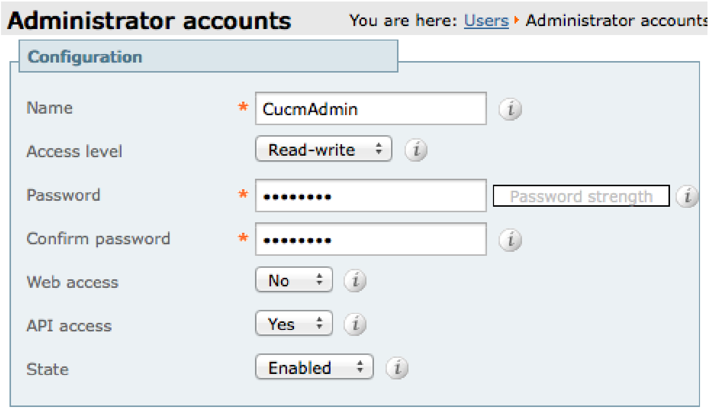
Step 1: Log into TelePresence Conductor as a user with administrator rights.

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

Step 3: Click **New**.

Step 4: Enter the following in the relevant fields:

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



Administrator accounts

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

Step 5: Click **Save**.

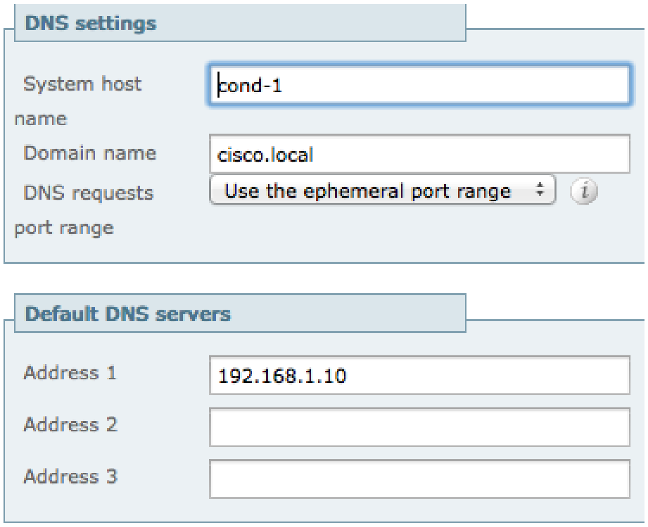
Procedure 2 Change the system settings

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

- System host name—**cond1**
- Domain name—**cisco.local**
- Address 1—**192.168.1.10**

Tech Tip

The FQDN of TelePresence Conductor will be **cond1.cisco.local**



DNS settings

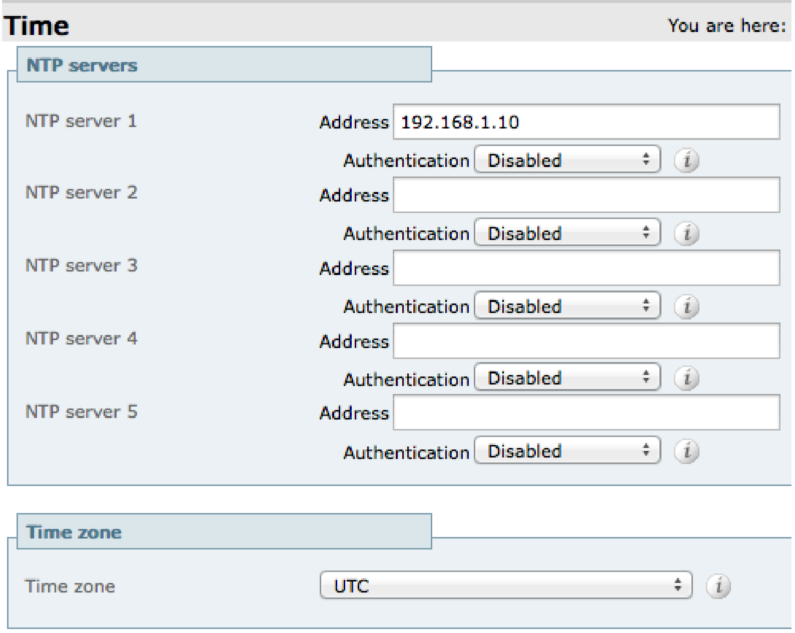
System host name	cond-1
Domain name	cisco.local
DNS requests port range	Use the ephemeral port range

Default DNS servers

Address 1	192.168.1.10
Address 2	
Address 3	

Step 2: Click **Save**.

Step 3: Navigate to **System** > **Time** and set **NTP server 1** to **192.168.1.10.**



Time You are here:

NTP servers

NTP server 1 Address 192.168.1.10
Authentication Disabled

NTP server 2 Address
Authentication Disabled

NTP server 3 Address
Authentication Disabled

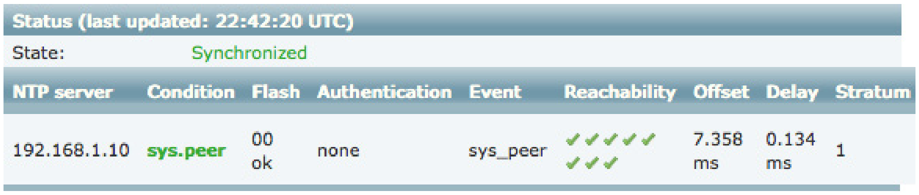
NTP server 4 Address
Authentication Disabled

NTP server 5 Address
Authentication Disabled

Time zone

Time zone UTC

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



Status (last updated: 22:42:20 UTC)

State: Synchronized

NTP server	Condition	Flash	Authentication	Event	Reachability	Offset	Delay	Stratum
192.168.1.10	sys.peer	00 ok	none	sys_peer	✓✓✓✓✓✓✓✓	7.358 ms	0.134 ms	1

Procedure 3 Add IP addresses for ad-hoc and rendezvous locations on Conductor

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

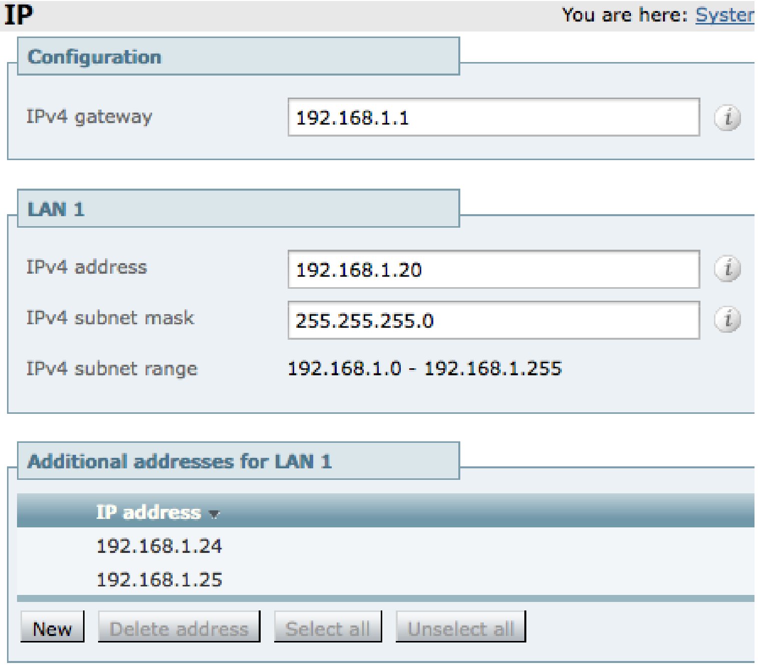
Step 2: Add the IP addresses used for ad-hoc conferences (**192.168.1.25**) and click **Add Address**.

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 rendezvous conferences (**192.168.1.24**) and click **Add address**:

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



IP

You are here: Syster

Configuration

IPv4 gateway: 192.168.1.1

LAN 1

IPv4 address: 192.168.1.20

IPv4 subnet mask: 255.255.255.0

IPv4 subnet range: 192.168.1.0 - 192.168.1.255

Additional addresses for LAN 1

IP address
192.168.1.24
192.168.1.25

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.

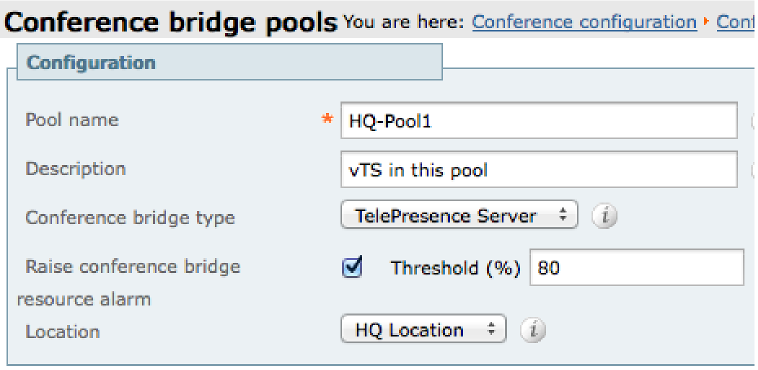
Procedure 4 Set up conference bridge pools

To set up a conference bridge pool, you need to create a conference bridge pool and then add the vTS 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**



Conference bridge pools

You are here: Conference configuration ▸ Conf

Configuration

Pool name *: HQ-Pool1

Description: vTS in this pool

Conference bridge type: TelePresence Server

Raise conference bridge resource alarm: ☑ Threshold (%) 80

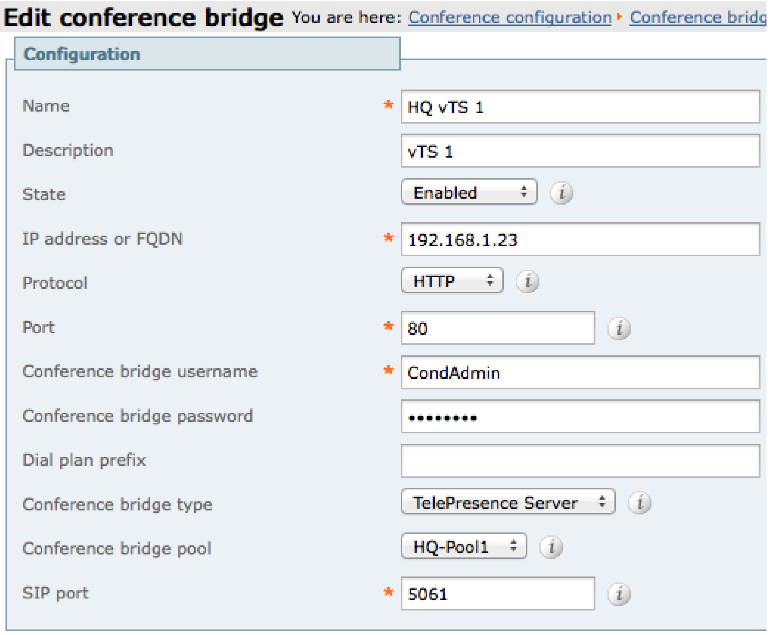
Location: HQ Location

Step 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–**192.168.1.23**
- Port–**80**
- Conference bridge username–**CondAdmin**
- Conference bridge password–**[password for the CondAdmin]**
- SIP port–**5061**



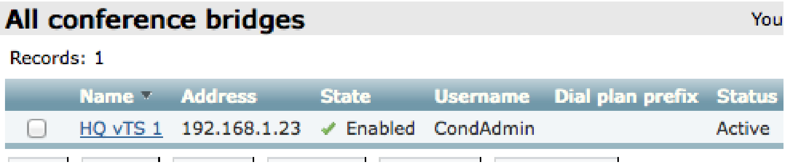
Edit conference bridge You are here: Conference configuration ▸ Conference bridg

Configuration

Name	*	HQ vTS 1
Description		vTS 1
State		Enabled
IP address or FQDN	*	192.168.1.23
Protocol		HTTP
Port	*	80
Conference bridge username	*	CondAdmin
Conference bridge password		••••••••
Dial plan prefix		
Conference bridge type		TelePresence Server
Conference bridge pool		HQ-Pool1
SIP port	*	5061

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

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



All conference bridges You

Records: 1

	Name	Address	State	Username	Dial plan prefix	Status
□	HQ vTS 1	192.168.1.23	✓ Enabled	CondAdmin		Active

Procedure 5 Create Service preferences

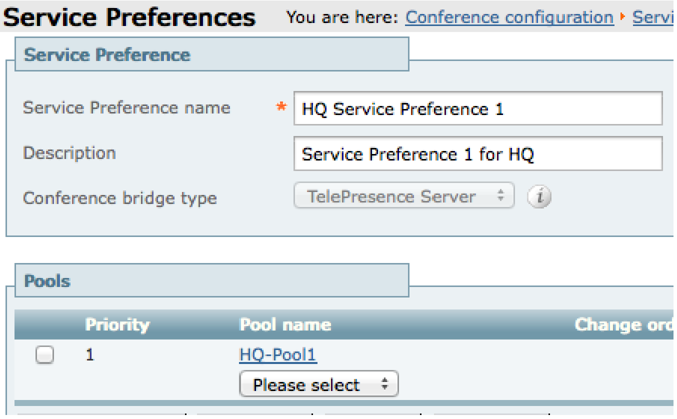
Step 1: Go to Conference configuration > Service Preferences.

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
- Pool name—**HQ-Pool1**

Step 4: Click Add selected pool.



Service Preferences

You are here: Conference configuration ▸ Servi

Service Preference

Service Preference name * HQ Service Preference 1

Description Service Preference 1 for HQ

Conference bridge type TelePresence Server

Pools

	Priority	Pool name	Change ord
□	1	HQ-Pool1 Please select	

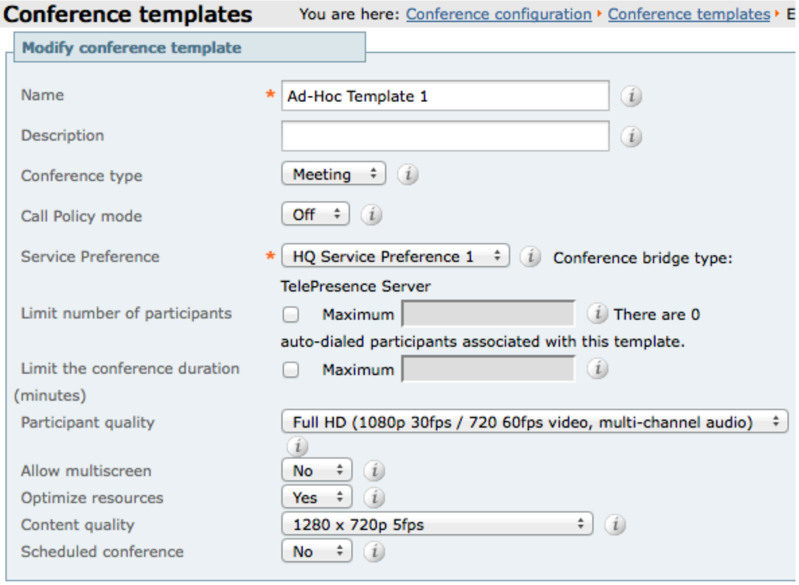
Step 5: Click Save.

Procedure 6 Create a template for an ad hoc meeting-type 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—**Full HD**
- Optimize resources—**Yes**
- Content quality—**1280 x 720p 5fps**


Conference templates

You are here: Conference configuration ▸ Conference templates ▸ E

Modify conference template

Name *	Ad-Hoc Template 1
Description	
Conference type	Meeting
Call Policy mode	Off
Service Preference *	HQ Service Preference 1 Conference bridge type: TelePresence Server
Limit number of participants	□ Maximum There are 0 auto-dialed participants associated with this template.
Limit the conference duration (minutes)	□ Maximum
Participant quality	Full HD (1080p 30fps / 720 60fps video, multi-channel audio)
Allow multiscreen	No
Optimize resources	Yes
Content quality	1280 x 720p 5fps
Scheduled conference	No

Step 3: Configure other entries as required.

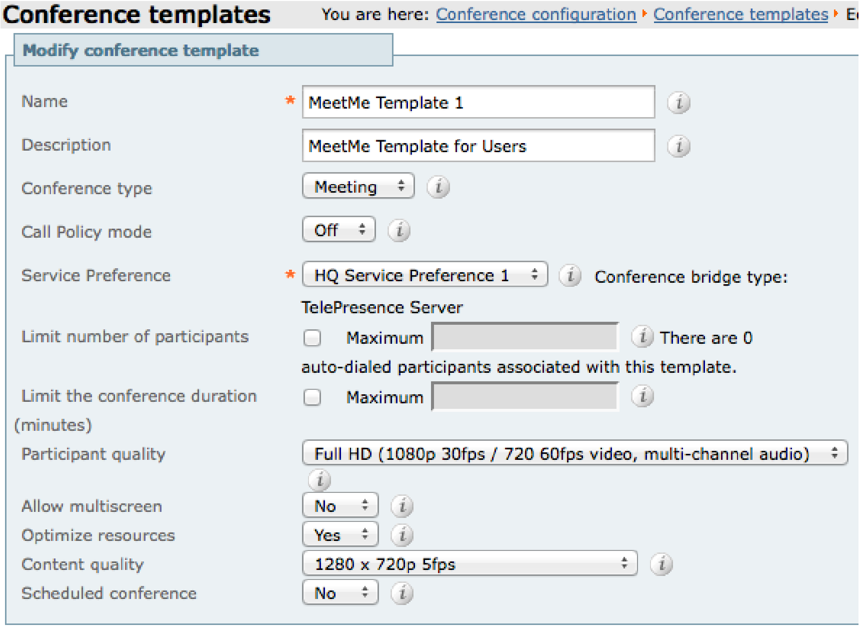
Step 4: Click **Create conference template**.

Procedure 7 Create a conference template for a rendezvous meeting-type 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—**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**



Conference templates You are here: Conference configuration ▸ Conference templates ▸ E

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 Conference bridge type: TelePresence Server
Limit number of participants	□ Maximum There are 0 auto-dialed participants associated with this template.
Limit the conference duration (minutes)	□ Maximum
Participant quality	Full HD (1080p 30fps / 720 60fps video, multi-channel audio)
Allow multiscreen	No
Optimize resources	Yes
Content quality	1280 x 720p 5fps
Scheduled conference	No

Step 3: Configure other entries as required.

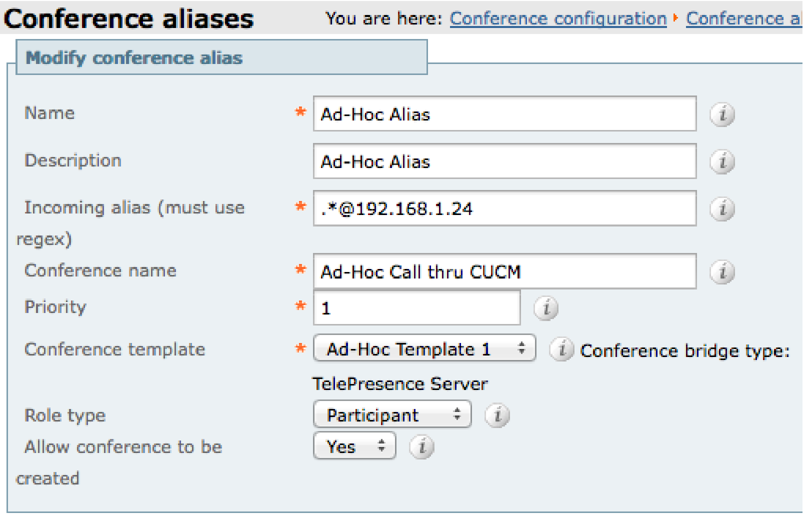
Step 4: Click **Create conference template**.

Procedure 8 Create a conference alias for an ad-hoc 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—**Ad-Hoc Alias**
- Incoming Alias (must use regex)—**.*@192.168.1.24**
- Conference name—**Ad-Hoc Call thru CUCM**
- Priority—**1**
- Conference template—Ad-Hoc Template 1
- Role type—Participant
- Allow conference to be created—Yes



Conference aliases You are here: Conference configuration ▸ Conference a

Modify conference alias

Name	*	Ad-Hoc Alias
Description		Ad-Hoc Alias
Incoming alias (must use regex)	*	.*@192.168.1.24
Conference name	*	Ad-Hoc Call thru CUCM
Priority	*	1
Conference template	*	Ad-Hoc Template 1 Conference bridge type: TelePresence Server
Role type		Participant
Allow conference to be created		Yes

Step 3: Click Create conference alias.

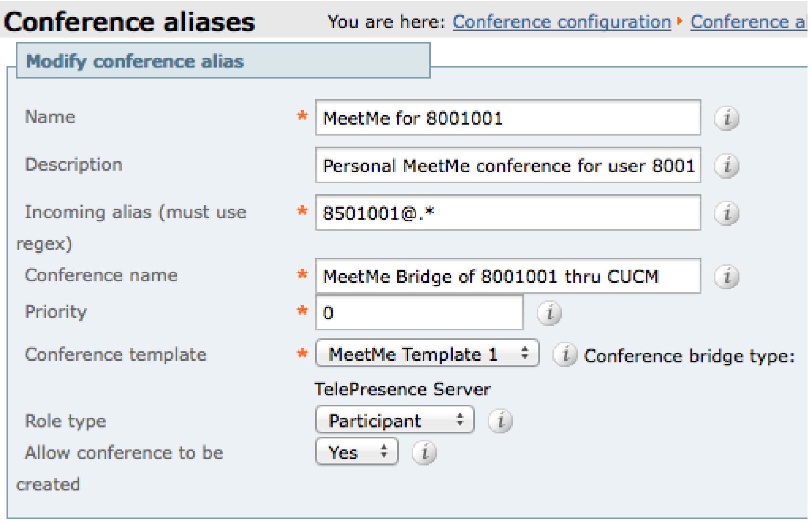
Procedure 9 Create a conference alias for a rendezvous conference

Create individual rendezvous conference aliases for every user.

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 8001001**
- Incoming Alias (must use regex)—**8501001@.***
- Conference name—**MeetMe Bridge of 8001001 thru CUCM**
- Priority—**0**
- Conference template—MeetMe Template 1
- Role type—Participant
- Allow conference to be created—Yes



Conference aliases You are here: Conference configuration ▸ Conference a

Modify conference alias

Name	*	MeetMe for 8001001
Description		Personal MeetMe conference for user 8001
Incoming alias (must use regex)	*	8501001@.*
Conference name	*	MeetMe Bridge of 8001001 thru CUCM
Priority	*	0
Conference template	*	MeetMe Template 1 Conference bridge type: TelePresence Server
Role type		Participant
Allow conference to be created		Yes

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

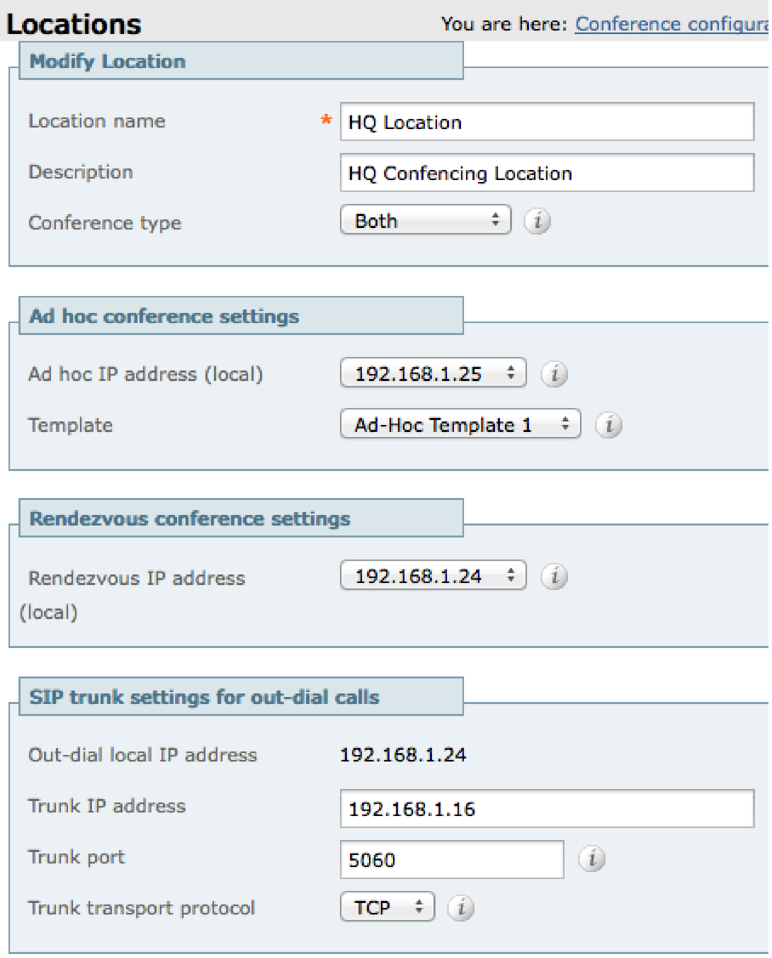
Step 4: Create additional conference aliases for all the users.

Procedure 10 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)—**192.168.1.25**
- Template—Ad-Hoc Template 1
- Rendezvous IP address (local)—**192.168.1.24**
- Trunk IP address—**192.168.1.16**
- Trunk port—**5060**
- Trunk transport protocol—TCP



Locations

You are here: Conference configura

Modify Location

Location name *	HQ Location
Description	HQ Confencing Location
Conference type	Both

Ad hoc conference settings

Ad hoc IP address (local)	192.168.1.25
Template	Ad-Hoc Template 1

Rendezvous conference settings

Rendezvous IP address (local)	192.168.1.24

SIP trunk settings for out-dial calls

Out-dial local IP address	192.168.1.24
Trunk IP address	192.168.1.16
Trunk port	5060
Trunk transport protocol	TCP

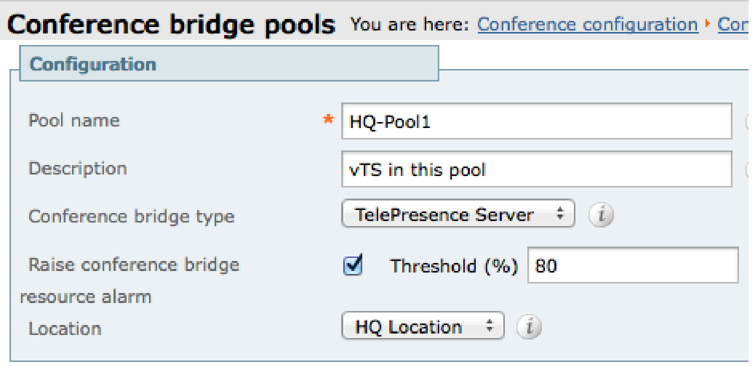
Step 3: Click Add location.

Procedure 11 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 then click **HQ-Pool1**.

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



Conference bridge pools You are here: Conference configuration ‣ Cor

Configuration

Pool name * HQ-Pool1

Description vTS in this pool

Conference bridge type TelePresence Server

Raise conference bridge resource alarm ☑ Threshold (%) 80

Location HQ Location

Step 4: Click on **Save**.

Tech Tip

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

PROCESS

Configuring CUCM

1. Configure CUCM connectivity to the LAN
2. Configure region for video
3. Configure device pool for video and add the video region
4. Configure CUCM trunk to Conductor for Rendezvous Conferences
5. Configure CUCM trunk to Conductor for Ad-Hoc Conferences
6. Configure CUCM route pattern
7. Configure Conductor as conference bridge
8. Configure MRG and MRGL for video and add Conductor to this MRG
9. Add this MRGL to the device profile for video
10. Configure CUCM redundancy

Procedure 1 Configure CUCM connectivity to the LAN

The CUCM can be connected to a Cisco Nexus switch in the data center.

Step 1: Using a user account that has the ability to make configuration changes, log in to the Nexus switch.

Step 2: If there is a previous configuration on the switch port where the CUCM is connected, remove the individual commands by issuing a **no** in front of each command in order to bring the port back to its default state.

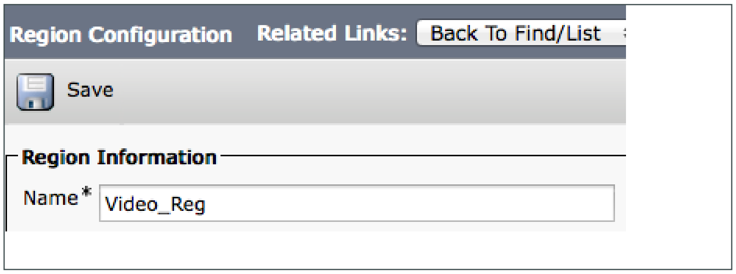
Step 3: Configure the port as an access port.

```
interface GigabitEthernet1/20
 description VCS
 switchport access vlan 20
 switchport host
```

Procedure 2 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.**

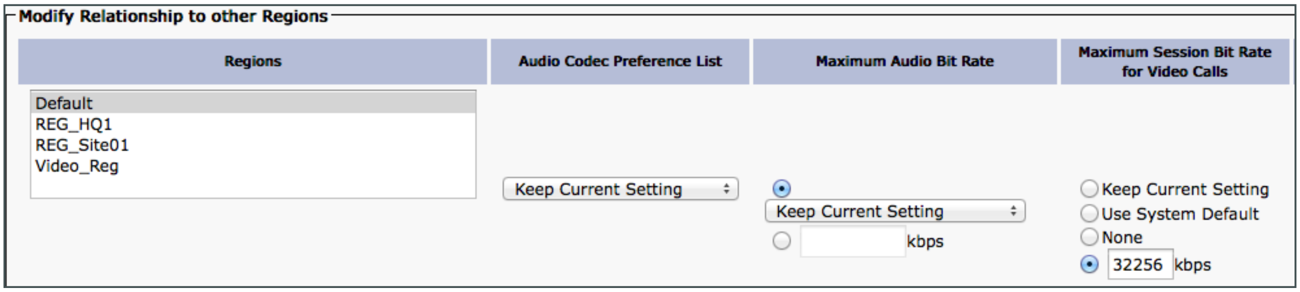


Region Information

Name* Video_Reg

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

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



Modify Relationship to other Regions

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default REG_HQ1 REG_Site01 Video_Reg	Keep Current Setting	● Keep Current Setting ○ kbps	○ Keep Current Setting ○ Use System Default ○ None ● 32256 kbps

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

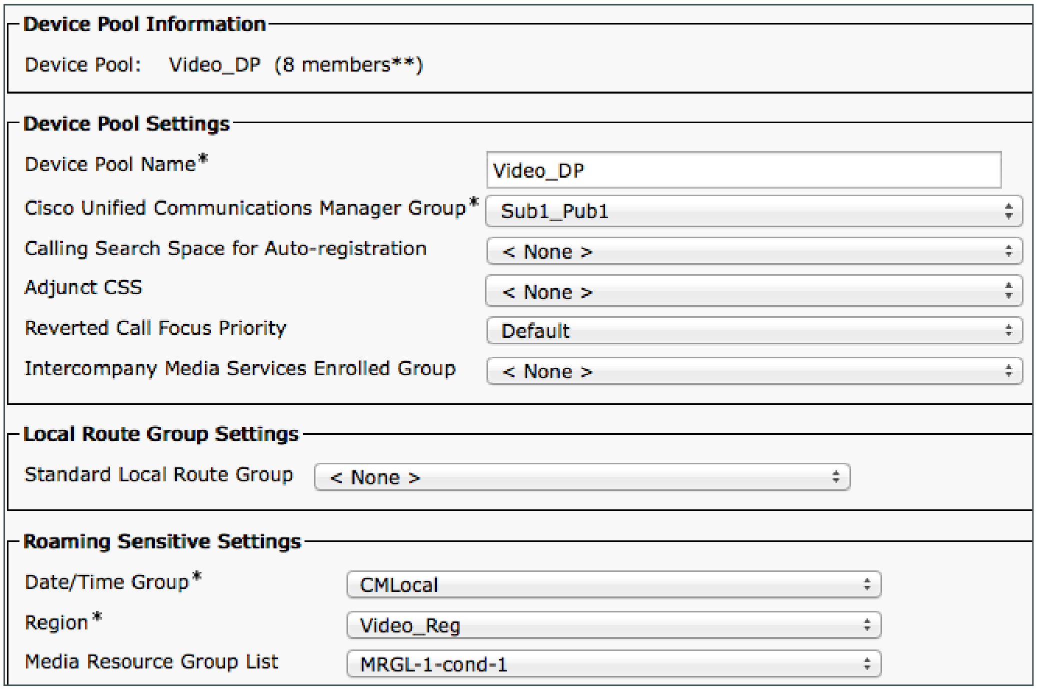
Step 5: Click **Save**.

Procedure 3 Configure device pool for video and add the video region

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

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

- Device Pool Name—**Video_DP**
- Region—**Video_Reg**



Device Pool Information

Device Pool: Video_DP (8 members**)

Device Pool Settings

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

Local Route Group Settings

Standard Local Route Group	< None >

Roaming Sensitive Settings

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

Step 3: Click **Save**.

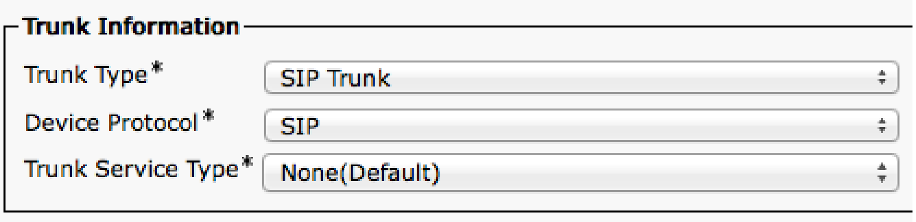
Procedure 4 Configure CUCM trunk to Conductor for Rendezvous Conferences

A *trunk* is a communications channel on Cisco Unified Communications Manager (Unified CM) that enables Unified CM 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)**



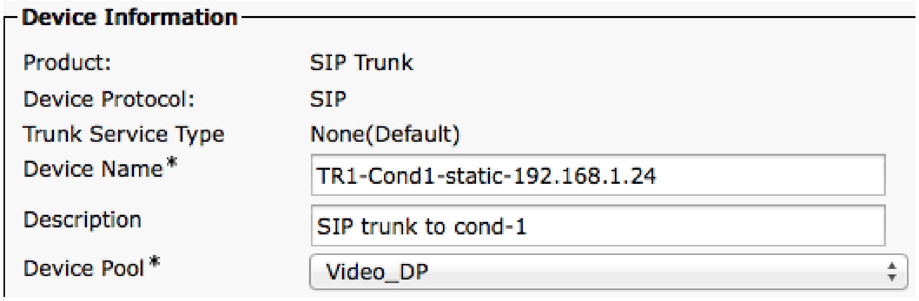
Trunk Information

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

Step 3: Click **Next**.

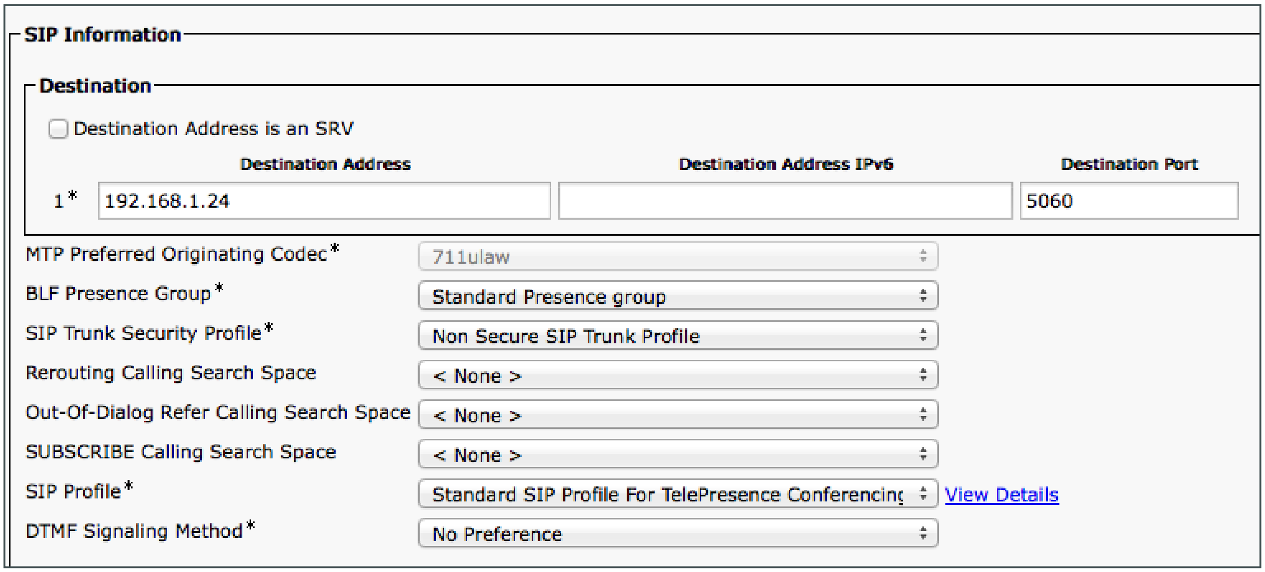
Step 4: Enter the following into the relevant fields, leaving other fields at their default values:

- Device Name—**TR1-Cond1-static-192.168.1.24**
- Device Pool—**Video_DP**
- Destination Address—**192.168.1.24**
- 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-192.168.1.24
Description	SIP trunk to cond-1
Device Pool*	Video_DP



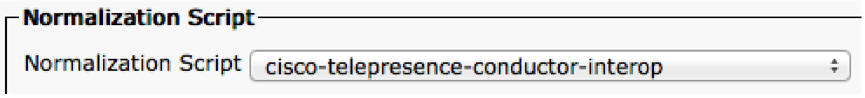
SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	192.168.1.24		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**.

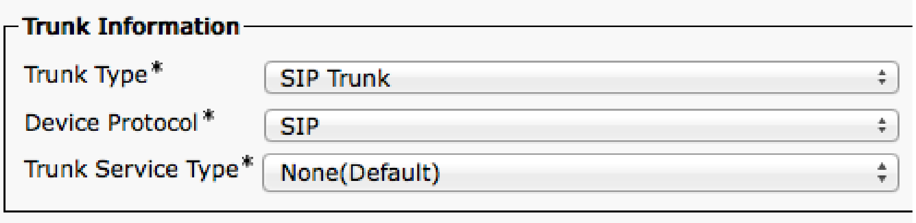
Step 6: Click **Reset**.

Procedure 5 Configure CUCM trunk to Conductor for Ad-Hoc 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)**



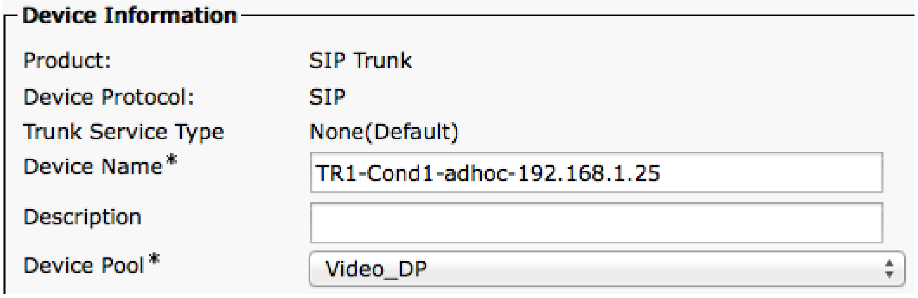
Trunk Information

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

Step 3: Click **Next**.

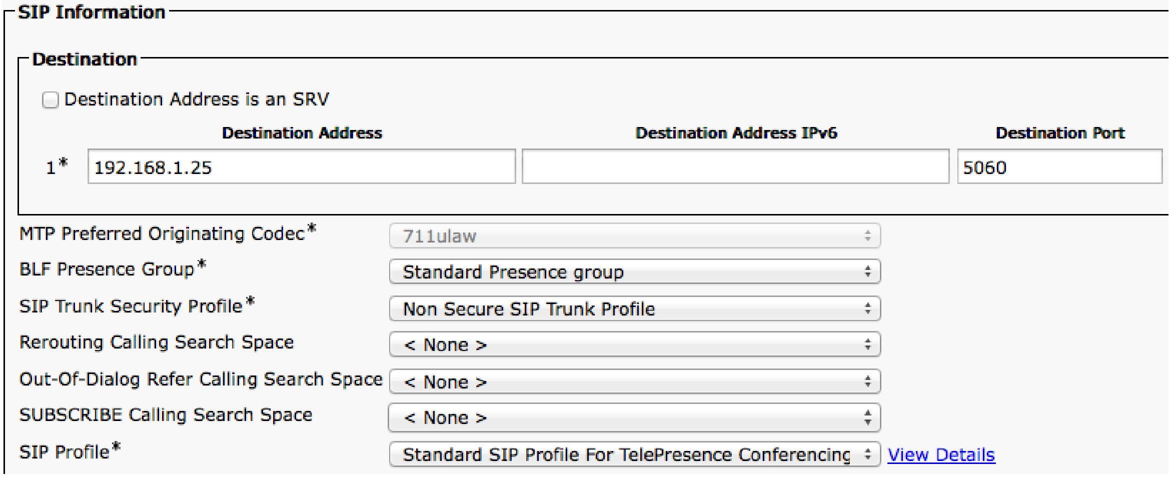
Step 4: Enter the following into the relevant fields, leaving other fields at their default values:

- Device Name—**TR1-Cond1-adhoc-192.168.1.25**
- Device Pool—**Video_DP**
- Destination Address—**192.168.1.25**
- Destination Port—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile**
- SIP Profile—**Standard SIP Profile for TelePresence Conferencing**



Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TR1-Cond1-adhoc-192.168.1.25
Description	
Device Pool*	Video_DP



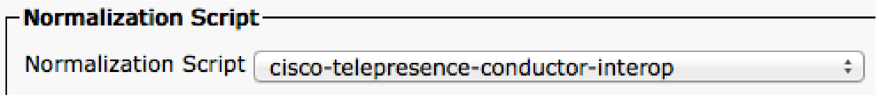
SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	192.168.1.25		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



Normalization Script

Normalization Script: cisco-telepresence-conductor-interop

Step 5: Click **Save**.

Click **Reset**.

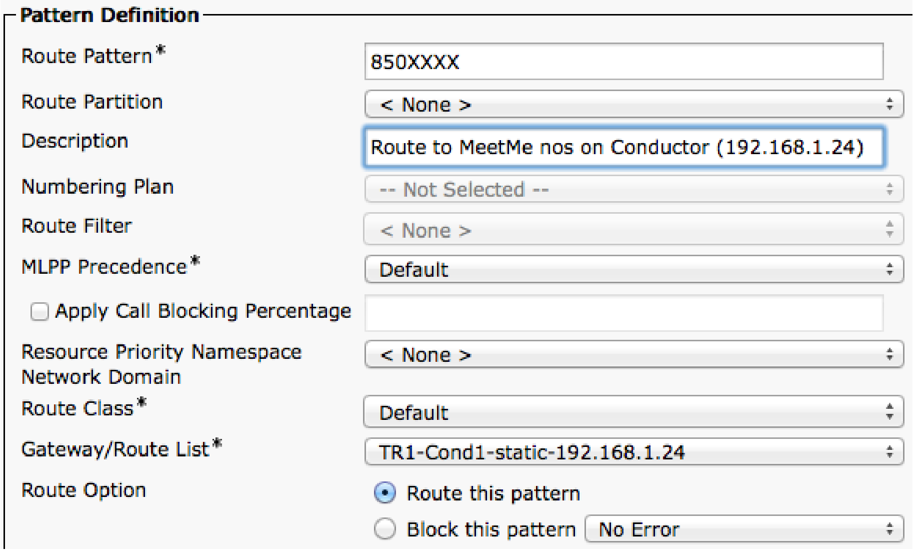
Procedure 6 Configure CUCM route pattern

This procedure describes configuring the CUCM route pattern to match the SIP trunk to TelePresence Conductor for rendezvous meetings.

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

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

- Route Pattern—**850XXXX**
- Gateway/Route List—**TR1-Cond1-static-192.168.1.24**



Pattern Definition

Route Pattern*	850XXXX
Route Partition	< None >
Description	Route to MeetMe nos on Conductor (192.168.1.24)
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	TR1-Cond1-static-192.168.1.24
Route Option	● Route this pattern ○ Block this pattern No Error

Step 3: Click **Save**.

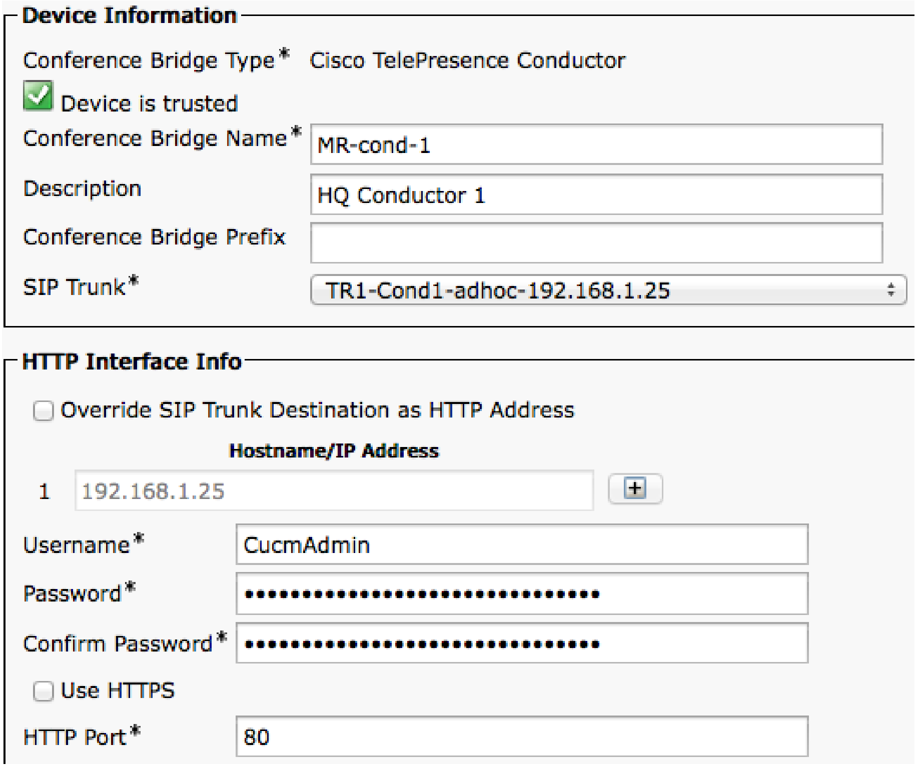
Procedure 7 Configure Conductor as conference bridge

This procedure describes configuring Conductor as a conference bridge in CUCM for ad-hoc 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-192.168.1.25**
- Override SIP Trunk Destination as HTTP Address—UnSelected
- Username—**CucmAdmin**
- Password—**<password for CucmAdmin created in Conductor>**
- HTTP Port—**80**



Device Information

Conference Bridge Type* Cisco TelePresence Conductor

☑ Device is trusted

Conference Bridge Name*	MR-cond-1
Description	HQ Conductor 1
Conference Bridge Prefix	
SIP Trunk*	TR1-Cond1-adhoc-192.168.1.25

HTTP Interface Info

□ Override SIP Trunk Destination as HTTP Address

	Hostname/IP Address
1	192.168.1.25

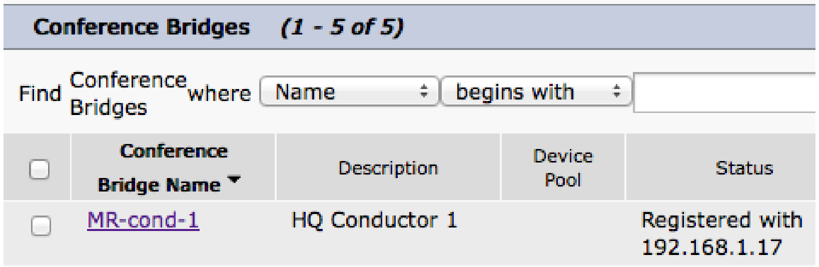
Username*	CucmAdmin
Password*	••••••••••••••••••••••••••••••••
Confirm Password*	••••••••••••••••••••••••••••••••

□ Use HTTPS

HTTP Port*	80

Step 3: Click **Save**.

Step 4: Make sure that the Conference Bridge shows as registered to the CUCM.



Conference Bridges ***(1 - 5 of 5)***

Find Conference Bridges where Name begins with

□	Conference Bridge Name ▾	Description	Device Pool	Status
□	MR-cond-1	HQ Conductor 1		Registered with 192.168.1.17

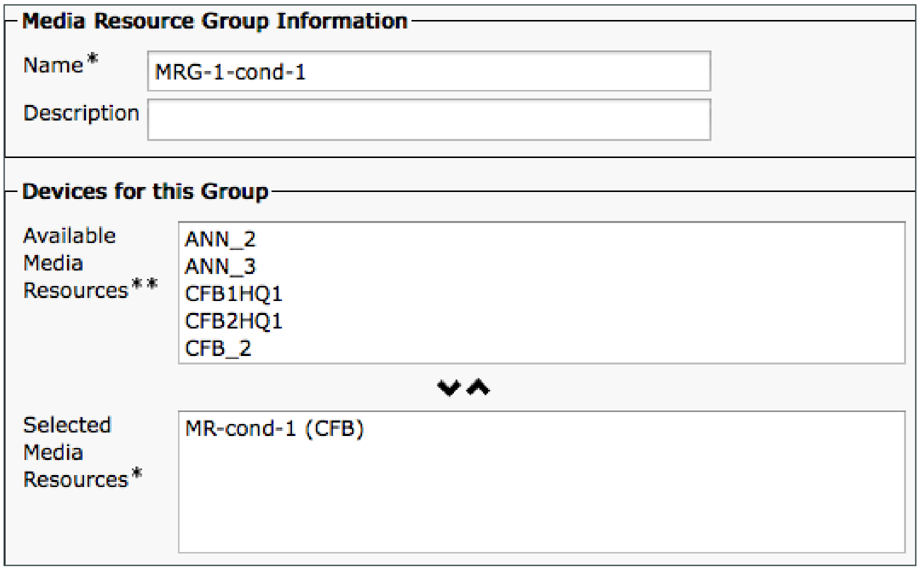
Procedure 8 Configure MRG and MRGL for video and add Conductor to this MRG

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

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

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

Step 4: Click **Save**.



Media Resource Group Information

Name* MRG-1-cond-1

Description

Devices for this Group

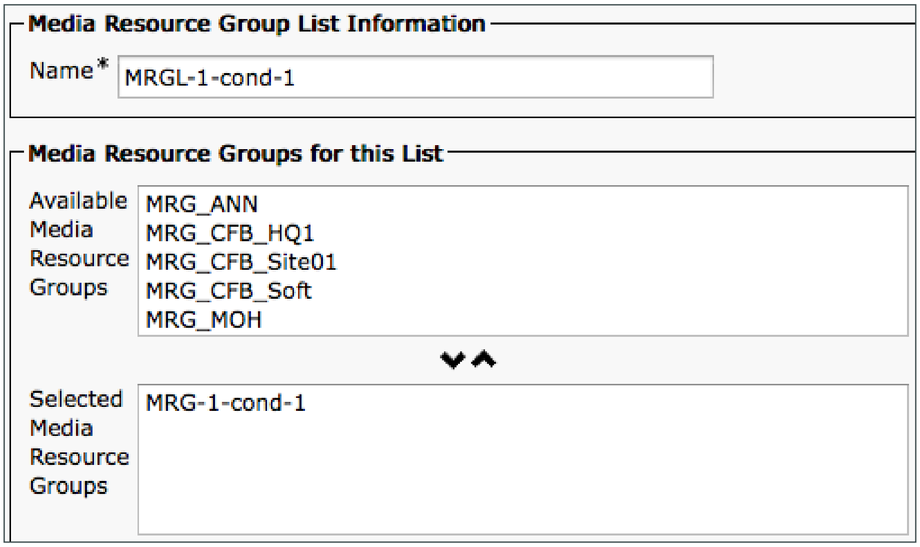
Available Media Resources** ANN_2
ANN_3
CFB1HQ1
CFB2HQ1
CFB_2

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

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

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

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



Media Resource Group List Information

Name* MRGL-1-cond-1

Media Resource Groups for this List

Available Media Resource Groups: MRG_ANN
MRG_CFB_HQ1
MRG_CFB_Site01
MRG_CFB_Soft
MRG_MOH

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

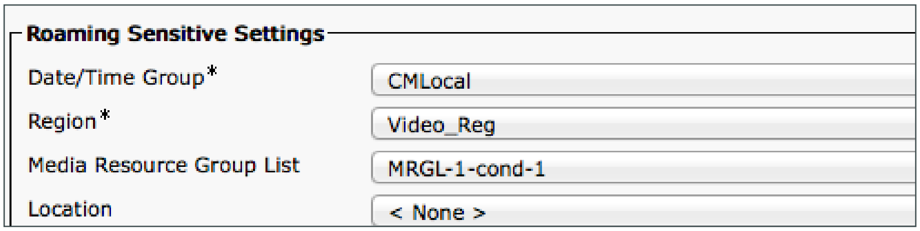
Step 8: Click **Save**.

Procedure 9 Add this MRGL to the device profile for video

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

Step 2: Select **Video_DP**.

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



Roaming Sensitive Settings

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

Step 4: Click **Save**.

Procedure 10 Configure CUCM redundancy

Please refer Unified Communications using Cisco BE 6000 Technology Design Guide document for guidance on redundancy.

PROCESS

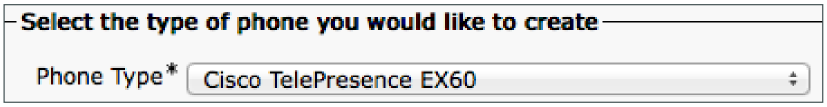
Configuring Endpoints

1. Configure CUCM for endpoints
2. Configure EX series
3. Configure SX20

Procedure 1 Configure CUCM for endpoints

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

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



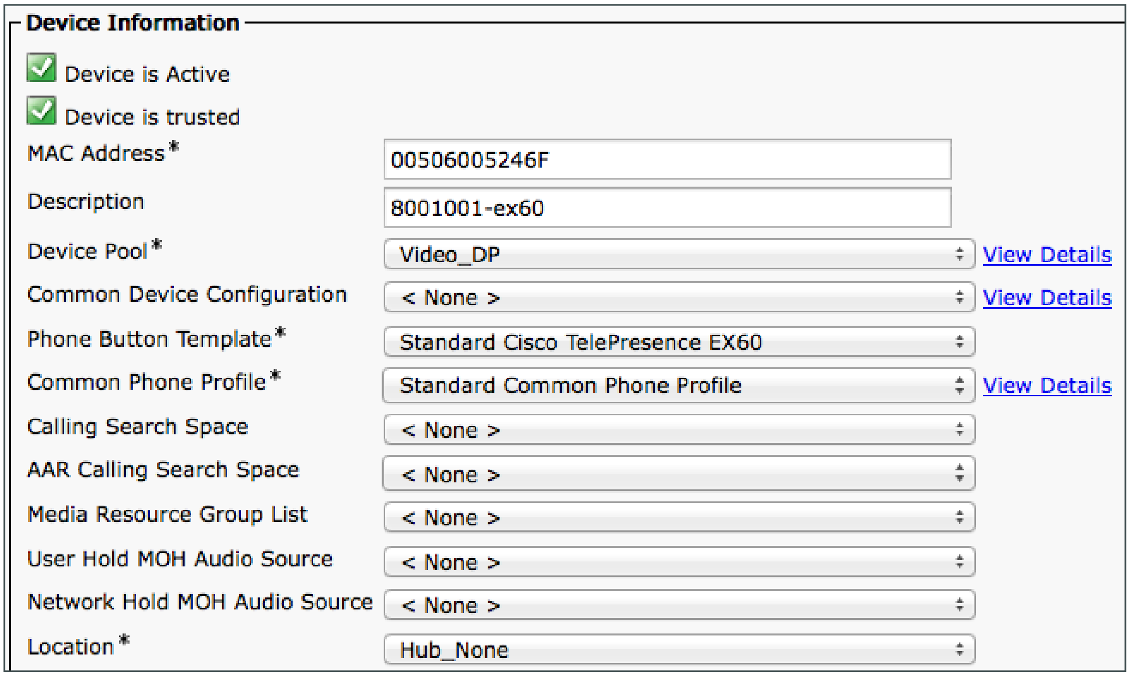
Select the type of phone you would like to create

Phone Type*	Cisco TelePresence EX60

Step 3: Click **Next**.

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

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

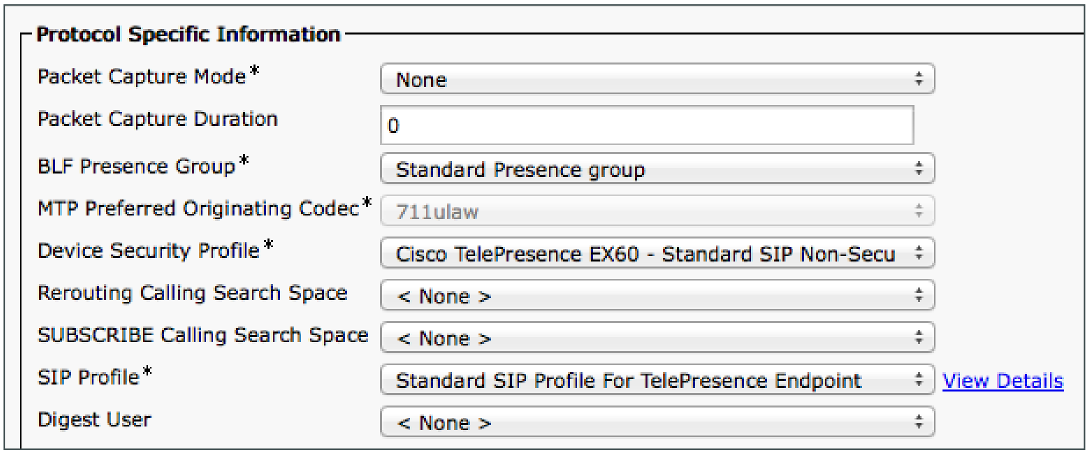


Device Information

☑ Device is Active

☑ Device is trusted

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

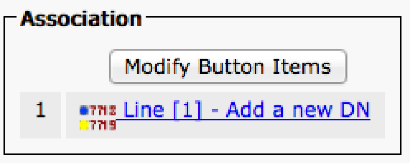


Protocol Specific Information

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

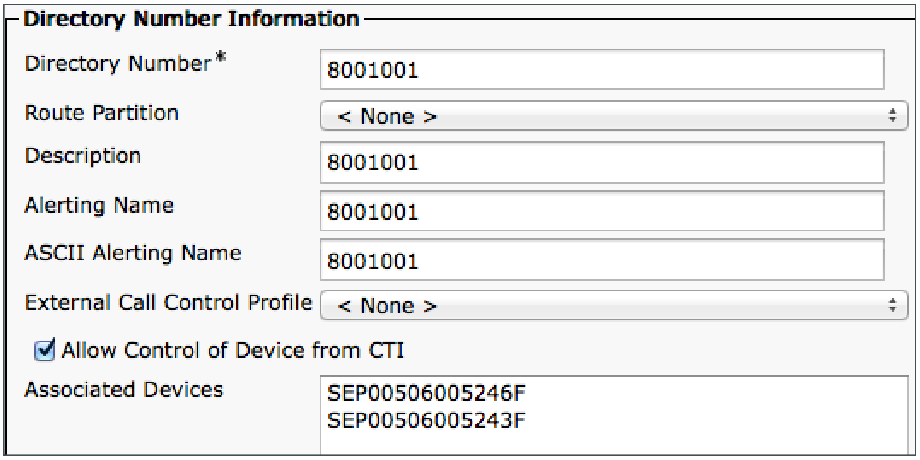
Step 5: Click **Save**.

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



Association

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



Directory Number Information

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

Step 8: Click **Apply Config**.

Procedure 2 Configure EX series

Step 1: Navigate to **Settings Icon > Administrator > Provisioning**, and then click **Start**.

Step 2: Select **Cisco UCM**, and then click **Next**.

Step 3: Select **Delete old certificate files (CTL, ITL)**.

Step 4: In **External Manager**, enter **192.168.1.16**, and then click **Register.**

Procedure 3 Configure SX20

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

Step 2: In **External Manager**, enter **192.168.1.16**, and then click **Save.**

PROCESS

Initiating Conferences

1. Initiate ad-hoc conference
2. Initiate rendezvous conference

Procedure 1 Initiate ad-hoc 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 ad-hoc conference should be connected.

Procedure 2 Initiate rendezvous conference

Step 1: Call **8501001** from **8001001**.

Step 2: Call **8501001** from **8001003**.

Step 3: Call **8501001** from **8001003**.

The rendezvous conference should be connected.

Appendix A: Product List

Component	Product Description	Part Number	Software
Call Control	Cisco Business Edition 6000 with up to 1000 users	BE6K-ST-BDL-K9 BE6K-STBDL-PLS-K9	10.0
Video Phones	Unified IP Phones 9900 series and DX600 series	CP-9971-C-K9	sip9971.9-4-1-9
	Unified IP Phones DX600 series	CP-DX650-K9	sipdx650.10-1-1-78
Video Endpoints	Cisco TelePresence EX series	CTS-EX90-K9	TC 7.0
	Cisco TelePresence SX series	CTS-SX20-PHD4X-K9	TC 7.0
Conference Bridge Controller	Mid Market Virtual TelePresence Conductor	R-VMCNDTRM-K9	2.2.1
Video Conference Bridge	Virtual TelePresence Server	R-VTS-K9	3.1
Video Conference Bridge UCS Server	Cisco UCS C240	UCSC-EZ-C240-109	N/A
Soft Client	Cisco Jabber for Windows	JAB9-DSK-K9	9.6

Feedback

Please use the feedback form to send comments and suggestions about this guide.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

B-445-COL-1 02/14