Cisco TelePresence Conductor with Cisco Unified Communications Manager

Deployment Guide

TelePresence Conductor XC4.0
Unified CM 10.5(2)

January 2016

Contents

Introduction **6**

About this document 6

Related documentation 6

About Cisco TelePresence Conductor and Cisco Unified Communications Manager 7

Unified CM / TelePresence Conductor connections 9

Call flow with the TelePresence Conductor 10

Ad hoc call flow 10

Rendezvous call flow 11

Example network deployment **12**

Cisco TelePresence network elements 12

Unified CM 12

Conference bridges 12

Endpoints 12

Prerequisites **13**

Configuring the TelePresence MCU **15**

Task 1: Resetting TelePresence MCU configuration to default 15

Task 2: Creating a user 15

Task 3: Installing an encryption key 16

Task 4: Configuring SIP 17

Task 5: Disabling H.323 registration 18

Task 6: Changing miscellaneous settings 19

Configuring the TelePresence Server **20**

Task 7: Creating a user 20

Task 8: Installing an encryption key 20

Task 9: Configuring SIP 22

Task 10: Disabling H.323 registration 24

Task 11: Configuring the operation mode 24

Configuring the TelePresence Conductor **26**

Configuring general settings on TelePresence Conductor 26

Task 12: Changing the administrator password 26

Task 13: Changing the root password 26

Task 14: Creating a user for Unified CM access 27

Task 15: Changing the system settings 28

Task 16: Setting up conference bridge pools 29
Task 17: Creating Service Preferences 33
Task 18: Adding IP addresses for ad hoc and rendezvous locations on TelePresence Conductor 35
Task 19: Adding FQDNs to server certificate 36
Configuring TelePresence Conductor for ad hoc conferences 36
Task 20: Creating a conference template for an ad hoc Meeting-type conference 37
Task 21: Creating an ad hoc Location 38
Configuring TelePresence Conductor for rendezvous conferences 39
Task 22: Creating a conference template for a rendezvous Meeting-type conference 39
Task 23: Creating a conference alias for a rendezvous Meeting-type conference 41
Task 24: Creating an auto-dialed participant for a rendezvous Meeting-type conference 42
Task 25: Creating a conference template for a rendezvous Lecture-type conference 43
Task 26: Creating a host conference alias for a rendezvous Lecture-type conference 45
Task 27: Creating a guest conference alias for a rendezvous Lecture-type conference 46
Task 28: Creating a rendezvous Location 47
Task 29: Adding Locations to conference bridge pools 49
Configuring Unified CM 50
Configuring general settings on Unified CM 50
Task 30: Viewing a location in Unified CM 50
Task 31: Ensuring that Unified CM trusts TelePresence Conductor's server certificate and vice versa 51
Task 32: Ensuring that a secure SIP trunk security profile is configured 52
Task 33: Creating a new SIP profile 53
Configuring Unified CM for ad hoc conferences 54
Task 34: Adding a SIP trunk connecting to TelePresence Conductor 54
Task 35: Adding the TelePresence Conductor as a Conference bridge to Unified CM 57
Task 36: Adding the TelePresence Conductor to an MRG and MRGL 59
Task 37: Adding an MRGL to a Device Pool or Device 60
Task 38: Adding the Unified CM normalization script 63
Configuring Unified CM for rendezvous conferences 63
Task 39: Adding a SIP trunk connecting to TelePresence Conductor 63
Task 40: Adding a route pattern to match the SIP trunk connecting to TelePresence Conductor 66
Task 41: Adding the Unified CM normalization script 67
Testing system configuration 68
Creating an ad hoc meeting 69
Creating a rendezvous meeting 71
Adding an auto-dialed participant 74

Checking cascading ... 74
Creating a system backup ... 76
Checking Unified CM message size limit ... 77
Troubleshooting ... 78
Viewing logs and calls on TelePresence Conductor ... 78
Viewing route information on Unified CM ... 78
Taking a trace on Unified CM using RTMT ... 79
Configure Unified CM to enable tracing ... 79
Installing RTMT – Real Time Monitoring Tool ... 79
Running RTMT ... 79
Taking a trace using RTMT ... 80
Specific issues ... 80
Unable to enable more than one conference bridge ... 80
TelePresence Conductor does not communicate with any conference bridges ... 80
Ad hoc call does not connect ... 81
Rendezvous call does not connect ... 82
Conference does not get created ... 82
Auto-dialed participant not connected ... 82
Auto-dialed participant disconnected when ad hoc conference is reduced to two parties ... 83
Guests are disconnected when hosts remain on the cascade MCU only ... 84
Conference name displayed on conference bridge is different from conference name that was configured ... 84
Duplicate display names ... 84
Only one screen of a multiscreen endpoint is used ... 85
CTS endpoint cannot join a conference on a TelePresence Server ... 86
Pre-configured endpoint cannot join conference ... 87
ActiveControl does not work on one or more endpoint(s) ... 88
Alarm "Invalid JSON found" raised for valid JSON string ... 88
Error messages ... 88
Regular expression match and replace ... 88
Appendix 1: Unified CM version 8.6.2 configuration ... 90
Adding TelePresence Conductor to Unified CM for ad hoc conferences ... 90
Appendix 2: Unified CM version 9.x configuration ... 92
Adding TelePresence Conductor to Unified CM for ad hoc conferences ... 92
Appendix 3: Adding the Unified CM normalization script ... 94

Appendix 4: Ensuring that Unified CM trusts TelePresence Conductor's server certificate and vice versa **96**
Loading server and trust certificates on TelePresence Conductor 96
Loading server and trust certificates on Unified CM 97
Appendix 5: Resilient deployment using clustered TelePresence Conductors **98**
Appendix 6: Multiparty Licensing **99**
Limitations 99
Feature support 99
Personal Multiparty 100
Configuration requirements 100
Configuration tasks 100
Tracking the number of licenses used 101
Appendix 7: Identifying dedicated content ports on a Cisco TelePresence MCU **102**
Document revision history **103**

Introduction

About this document

This document describes how to configure Cisco Unified Communications Manager to use a Cisco TelePresence Conductor to manage the conference bridge resources for ad hoc and rendezvous conferences. TelePresence Conductor configuration, TelePresence Server and TelePresence MCU configuration is also documented. Following the steps in this deployment guide will allow you to configure the above devices to allow:

- a Unified CM-registered endpoint to create an ad hoc conference by using its own “conference”, “join”, or “merge and accept” button to join multiple video participants together onto a conference bridge through a TelePresence Conductor.
- a Unified CM-registered endpoint to dial a specific dial string and create a rendezvous conference through a TelePresence Conductor on one or more of the conference bridges.

This document also describes how to check that the system is working as expected.

Descriptions of the system configuration parameters for the Unified CM, TelePresence Conductor and conference bridges can be found in the Administrator Guides and online help for each product. Both the Unified CM and the TelePresence Conductor web interfaces offer field help.

Related documentation

This document focuses on the key components needed for a Unified CM and TelePresence Conductor integration only. For more details on how to implement a Unified CM or a Unified CM cluster reference the Cisco Unified Communications Manager documentation on www.cisco.com.

For details on how to deploy a cluster of TelePresence Conductors with Unified CM see *Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide*.

This document describes how to configure the TelePresence Conductor with regex conference aliases using the web interface. If you are using Cisco TMSPE to provision collaboration meeting rooms (CMRs) omit the tasks that set up conference templates, conference aliases and auto-dialed participants on the TelePresence Conductor and instead follow *Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide*.

For details on how to deploy a TelePresence Conductor with a Cisco TelePresence Video Communication Server see either *Cisco TelePresence Conductor with Cisco VCS (Policy Service) Deployment Guide* or

Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide depending on the type of Cisco VCS deployment.

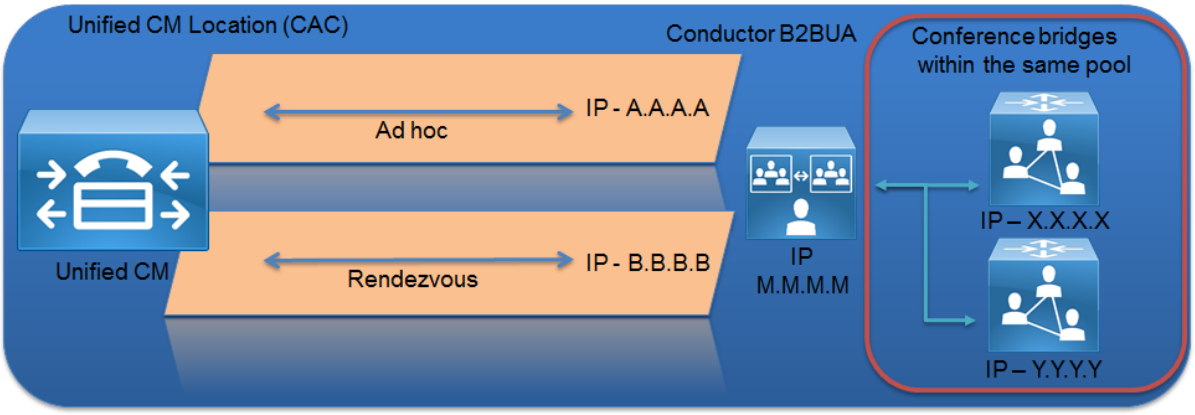
About Cisco TelePresence Conductor and Cisco Unified Communications Manager

In Unified CM version 8.6.2 Cisco introduced the ability to use a video MCU to handle ad hoc conferences using a mixture of XML RPC and SIP messaging. Rendezvous conferences are handled using a SIP trunk to a conference bridge. The rendezvous and ad hoc bridges, however, need to be separate physical bridges.

In version 9.x extensions to interoperation were added.

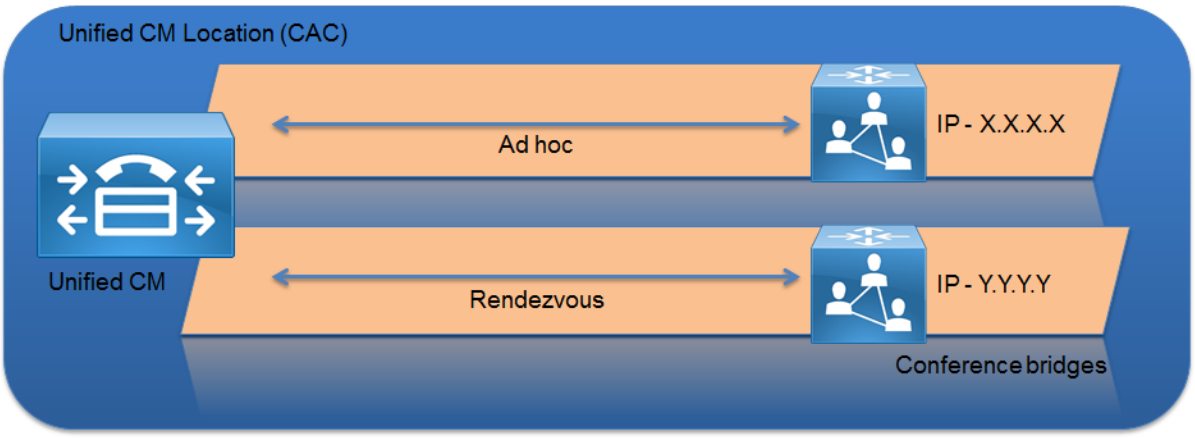
In version 10.x the configuration for ad hoc was modified.

We recommend that Unified CM version 10.x or later is used with TelePresence Conductor version XC4.0, although Unified CM versions 9.1.x and 8.6.2 will work. We also recommend configuring Unified CM to be configured to support SIP Early Offer (for further details see the latest *Cisco Collaboration Meeting Rooms (CMR) Premises Deployment Guide*).



TelePresence Conductor version XC4.0 can be configured to emulate conference bridges for Unified CM; using its back-to-back user agent (B2BUA) it can route the different types of conference calls (ad hoc or rendezvous) to one or more conference bridges. These bridges can be Cisco TelePresence MCUs or Cisco TelePresence Servers.

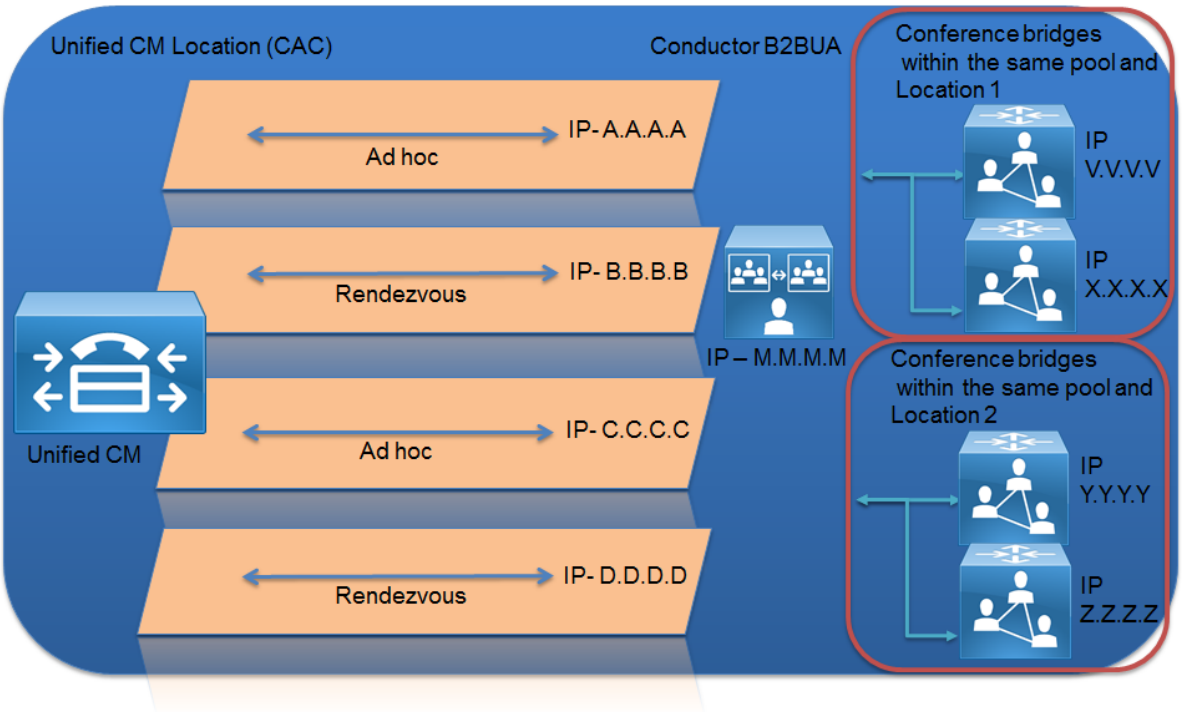
Without the TelePresence Conductor, Unified CM has to be configured to connect directly to the video multipoint control unit bridging resources.



With the TelePresence Conductor included, the ad hoc and rendezvous requests are received by the TelePresence Conductor and it can use both conference bridges for ad hoc and rendezvous calls, thus making more efficient use of the conference bridge resources available.

If Unified CM is configured to support Call Admission Control (CAC) policy to enforce bandwidth limitations, the TelePresence Conductor can be configured to support this. The TelePresence Conductor will need to be configured to only use conference bridges in the location that the ad hoc call or rendezvous call is made to.

In a design where a single Unified CM cluster or multiple Unified CM clusters support multiple CAC locations, the TelePresence Conductor must be configured with separate locations for each Unified CM CAC location where there are conferencing resources located. In addition, TelePresence Conductor must be configured to use conference bridge resources that are in the relevant Unified CM location; otherwise if this design is not followed the Unified CM CAC model will be broken.



Each TelePresence Conductor location will have a dedicated IP address for ad hoc conferences and another dedicated IP address for rendezvous conferences.

Note: The conference bridges to use for ad hoc conferences are defined by the template that is configured on the TelePresence Conductor's **Locations** page (Conference template > Service Preference > Conference bridge pools > Conference bridges). The conference bridges to use for rendezvous conferences are defined by the alias dialed (Conference alias > Conference template > Service Preference > Conference bridge pools > Conference bridges) – therefore for rendezvous conferences the prefix must be location specific.

TelePresence Conductor supports up to 30 Locations (limited by the 30 conference bridges that TelePresence Conductor supports).

Unified CM / TelePresence Conductor connections

For ad hoc conferences a SIP trunk is used from Unified CM to TelePresence Conductor. Set up the relevant TelePresence Conductor Location's ad hoc IP address as the destination of a SIP trunk on Unified CM. Ad hoc calls for that location can then be routed down that SIP trunk.

In addition to SIP messaging, ad hoc conferences also use XML RPC messaging. The destination for both SIP and XML RPC messages are configured (to the same TelePresence Conductor IP address) by configuring a Conference bridge in Unified CM. That Conference bridge will then be assigned to an MRG

(Media Resource Group), the MRG to an MRGL (Media Resource Group List), then the MRGL to a Device, either directly or by assigning the MRGL for use by a Device pool.

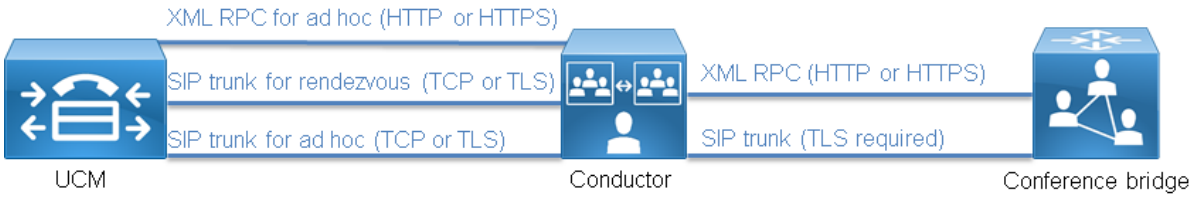
For rendezvous conferences a separate SIP trunk is used from Unified CM to TelePresence Conductor. Set up the relevant TelePresence Conductor Location's rendezvous IP address as the destination of a SIP trunk on Unified CM. Rendezvous calls for that location can then be routed down that SIP trunk.

For out-dialed calls from TelePresence Conductor to Unified CM, TelePresence Conductor will use the reverse path of the SIP Trunk used for rendezvous calls.

The SIP connections between Unified CM and TelePresence Conductor can either use TCP or TLS. The protocol configured in the TelePresence Conductor's Location must match the protocol configured in the Unified CM's SIP trunk security profile. We recommend that you use TLS and the example used in this guide therefore applies TLS settings.

The XML RPC connections between Unified CM and TelePresence Conductor can either use HTTP or HTTPS.

There are also SIP trunk and XML RPC connections between the TelePresence Conductor and the conference bridges. The XML RPC connections can be either HTTP or HTTPS, but the SIP trunks between TelePresence Conductor and the conference bridges must be TLS.



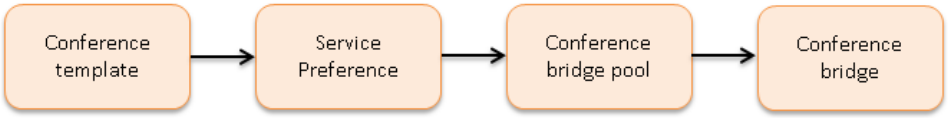
Call flow with the TelePresence Conductor

The following sections show the call flows that occur when handling ad hoc and rendezvous calls.

Ad hoc call flow

This diagram shows the call flow for an ad hoc call:

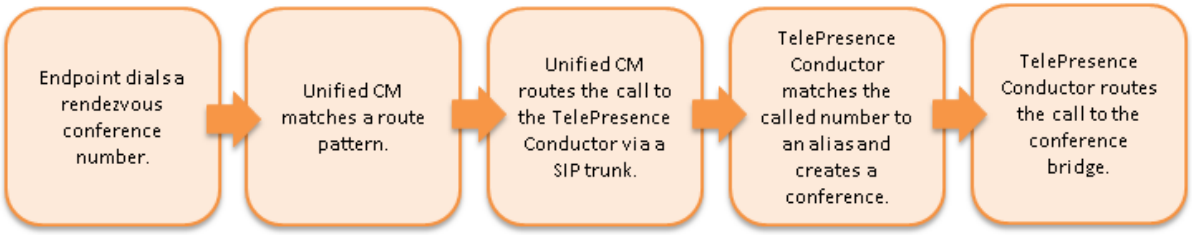
In TelePresence Conductor:



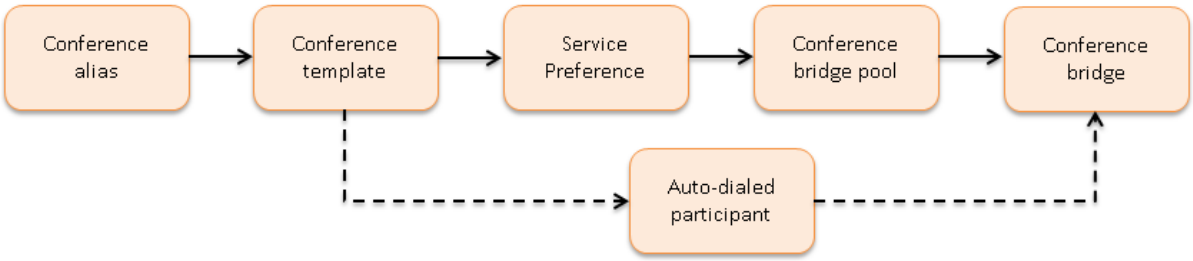
Once these parts of the call flow are complete, the calls are set up and media flows between the endpoints and the conference bridge.

Rendezvous call flow

This diagram shows the call flow for a rendezvous call:



In TelePresence Conductor:

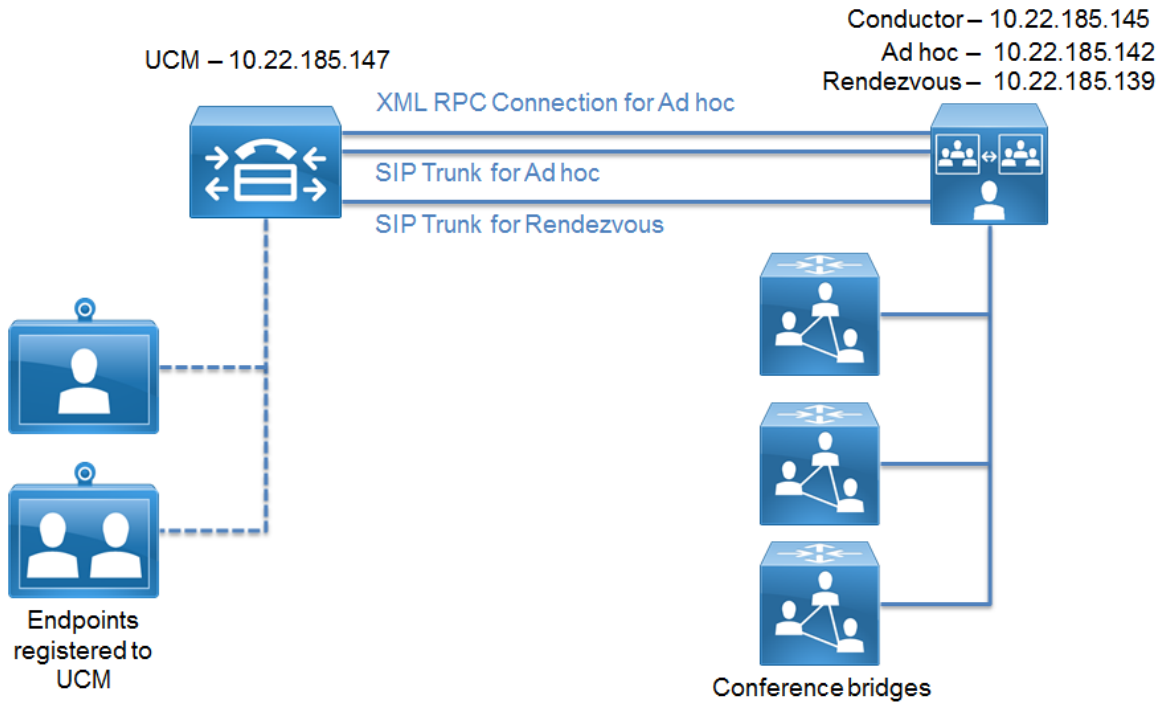


(The dotted line indicates an optional step where auto dialed participant(s) are configured on the TelePresence Conductor for the relevant template.)

Once these parts of the call flow are complete then the call is set up and media flows between the endpoints and the conference bridge.

Example network deployment

This document uses the example network shown in the diagram below as the basis for the deployment configuration described.



Cisco TelePresence network elements

Unified CM

The Unified CM acts as a call processor for routing voice and video device calls. It works with other infrastructure devices in the network to process call requests.

Conference bridges

Conference bridges are network devices that enable multiple video calls to come together in a multipoint video conference. TelePresence Conductor version XC4.0 supports the conference bridge types TelePresence MCU and TelePresence Server.

Endpoints

Endpoints are devices that receive and make video calls. They can be software clients on PCs and Macs such as Jabber, desktop endpoints such as the DX650 and EX90, or room systems such as the MX300.

Prerequisites

Before starting the system configuration, ensure you have met the following criteria:

- The Unified CM must already be configured with a base configuration and must be running Unified CM version 8.6.2 or later. We highly recommend that you use version 10.x or later. For details on Unified CM 8.6.2 configuration, refer to Appendix 1: Unified CM version 8.6.2 configuration [p.90]. For details on Unified CM 9.x configuration, refer to Appendix 2: Unified CM version 9.x configuration [p.92].
  Ensure connectivity by registering at least three endpoints to Unified CM, and make sure they are all capable of calling each other with voice and video communications. For more information, see the documentation on cisco.com under the Cisco Unified Communications Manager, http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.
- The TelePresence Conductor must be powered on, running version XC4.0 and accessible over the network. For assistance in reaching this stage see *Cisco TelePresence Conductor Administrator Guide*.
- The TelePresence Conductor must have enough unique IP addresses configured to fulfill the requirements for ad hoc and rendezvous type call configuration.
  The TelePresence Conductor will need, at minimum, an IP address for management plus an IP address for ad hoc conferences and another for rendezvous conferences. Additional IP addresses for ad hoc and rendezvous conferences will be required if multiple locations are handled.
- For ad hoc conferences, HTTP/HTTPS XML RPC messages and SIP INVITE messages must come from the same source IP address. This is used to match the incoming SIP call to the XML RPC message that started the conference.
- One or more conference bridges are powered on and accessible over HTTP/HTTPS and SIP TLS. Basic configuration for the conference bridge should be completed as described in the relevant Getting Started Guide. These bridges must be dedicated for use by the TelePresence Conductor – no other devices must try to route calls to them except via the TelePresence Conductor.
- The following Cisco TelePresence MCUs are supported by the TelePresence Conductor:
  - MCU 4200 series version 4.2 or later
  - MCU 4500 series version 4.2 or later
  - MCU 5300 series version 4.3(2.17) or later
  - MCU MSE 8420 version 4.2 or later
  - MCU MSE 8510 version 4.2 or later

  Note: for all TelePresence MCUs we recommend that you install the latest software version (4.5); otherwise some features will not be supported.

- The following Cisco TelePresence Servers are supported by the TelePresence Conductor:
  - TelePresence Server 7010 version 3.0(2.46) or later
  - TelePresence Server MSE 8710 version 3.0(2.46) or later
  - TelePresence Server version 3.1 or later on Virtual Machine
  - TelePresence Server version 3.1 on Multiparty Media 310/320

  Note: for all TelePresence Servers we recommend that you install the latest software version (4.1); otherwise some features will not be supported. TelePresence Server version 4.0(1.57) or later is required for cascading to work.
- This guide assumes the conference bridges are connected to the network on their port A.
- Endpoints are registered to Unified CM with the correct software versions.
- A web browser is available with access to the web interfaces of the Unified CM, TelePresence Conductor and conference bridges that are being configured.

Configuring the TelePresence MCU

The following tasks are required for both ad hoc and rendezvous conferences when using TelePresence MCUs as the conference bridges. You will need to repeat them for all TelePresence MCUs in the deployment.

The tasks are not required if only TelePresence Servers are used in the deployment.

Task 1: Resetting TelePresence MCU configuration to default

To ensure that all TelePresence MCUs used by this TelePresence Conductor have the same configuration settings applied, reset the TelePresence MCU configuration to its default values:

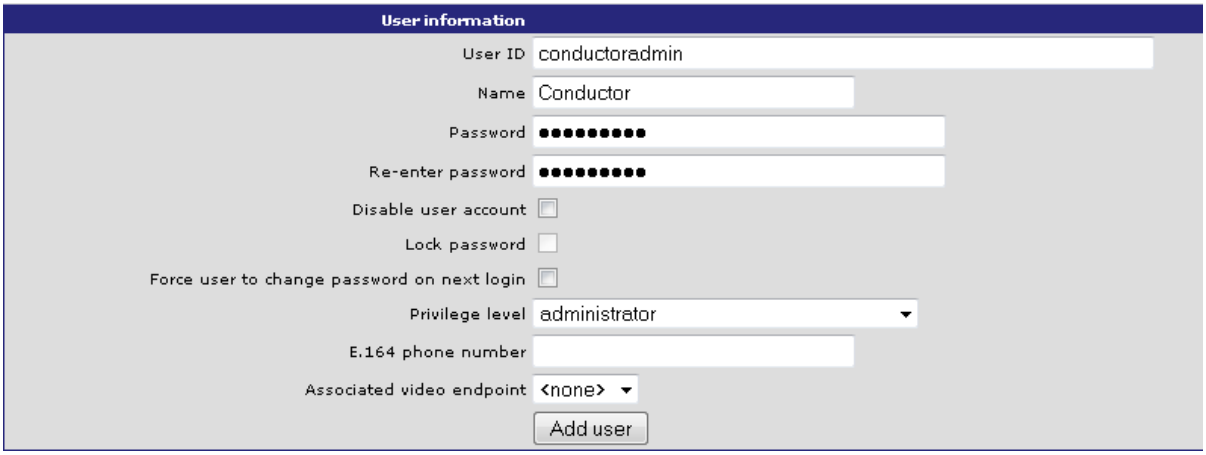
1. Create an xml file that only contains the following text:
   `<configuration/>`
2. Go to the web interface of the TelePresence MCU you want to configure and log in as an administrator.
3. Go to **Settings > Upgrade**.
4. In the **Restore configuration** section ensure that the **Overwrite settings** - **Network settings** and **User settings** - are NOT checked.
5. Next to **Backup file to be restored** click on **Choose File** and select the xml file you created earlier.
6. Click **Restore backup file**.
7. Go to **Settings > Shutdown** to shut down and subsequently restart the TelePresence MCU.

Task 2: Creating a user

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

1. On the TelePresence MCU go to **Users** and click **Add new user**.
2. Enter the following in the relevant fields:

User ID	Enter a username for the TelePresence Conductor to use.
Name	Enter a name for this user.
Password	Enter a password for the TelePresence Conductor to use.
Force user to change password on next login	Uncheck.
Privilege level	Select *administrator*.



3. Click **Add user**.

Task 3: Installing an encryption key

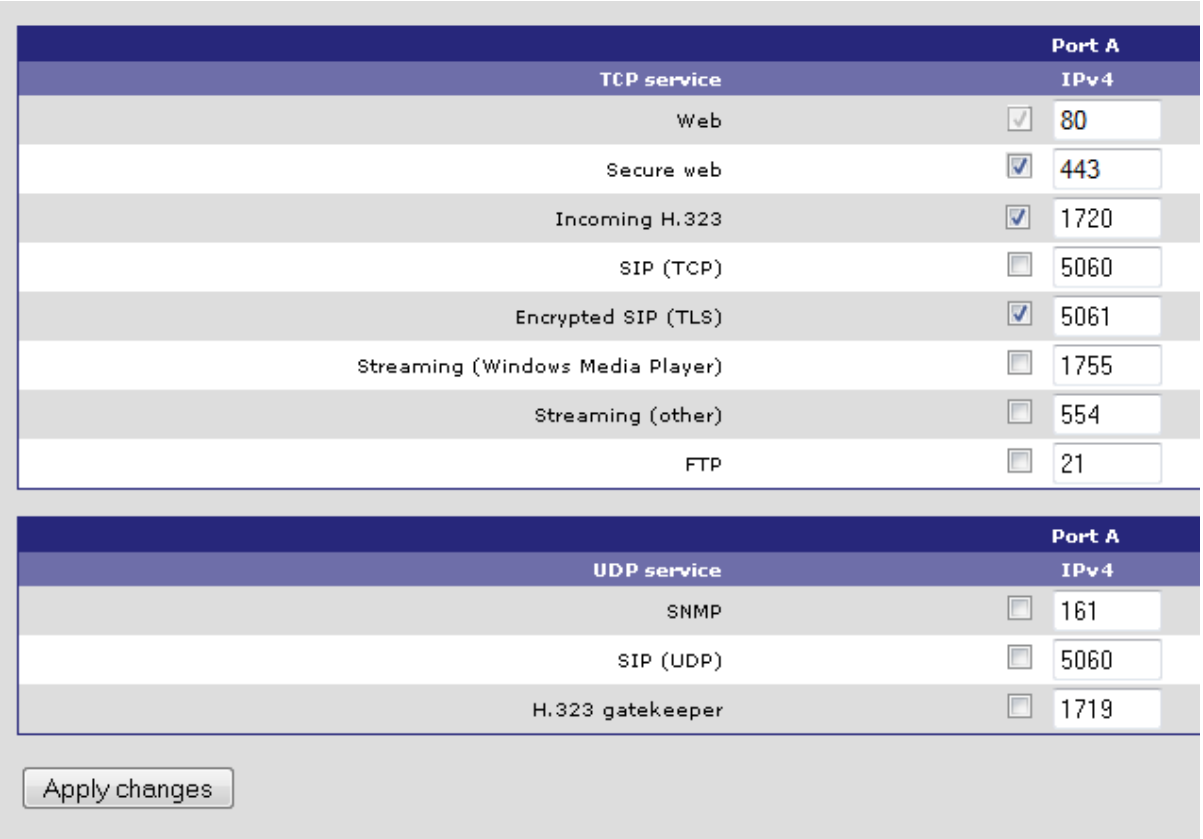
The TelePresence MCU has the ability to use a secure connection for communications. These security features are enabled with the **Encryption** option key. You must install the option key in order for this deployment to work.

To verify that the key is installed or to install the key:

1. Go to **Settings > Upgrade**.
2. Go to the **Feature Management** section and verify that the **Encryption key** is installed. If the key is not installed, enter the **Activation code** and click **Update features**.

To enable the use of encryption on the TelePresence MCU:

1. Go to **Settings > Encryption**.
2. Set **Encryption status** to *Enabled*.
3. Set **SRTP encryption** to *Secure transport (TLS) only*.
4. Click **Apply changes**.
5. Go to **Network > Services**.
6. Ensure that **Secure web (port 443)** is checked.
7. Ensure that **Incoming H.323** is checked. This is required for TelePresence MCU cascading to work.
8. Ensure that **SIP (TCP)** is unchecked.
9. Ensure that **Encrypted SIP (TLS)** is checked.
10. Ensure that **SIP (UDP)** is unchecked.

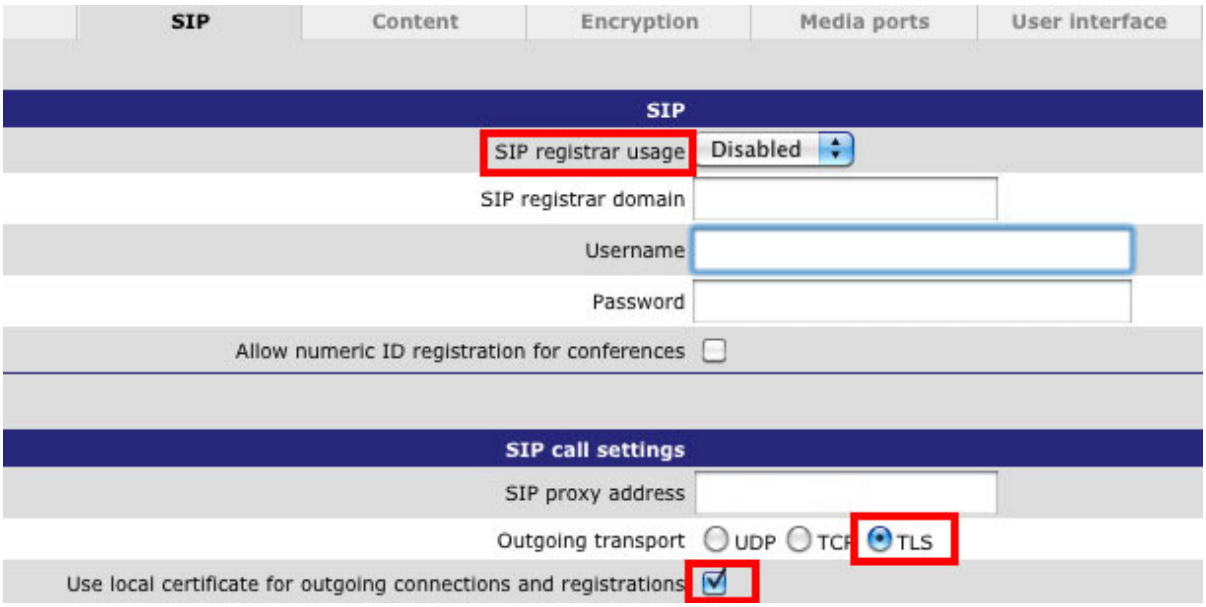


11. Click **Apply changes**.

Task 4: Configuring SIP

1. Go to **Settings > SIP**.
2. Enter the following into the relevant fields, leave other fields as their default values:

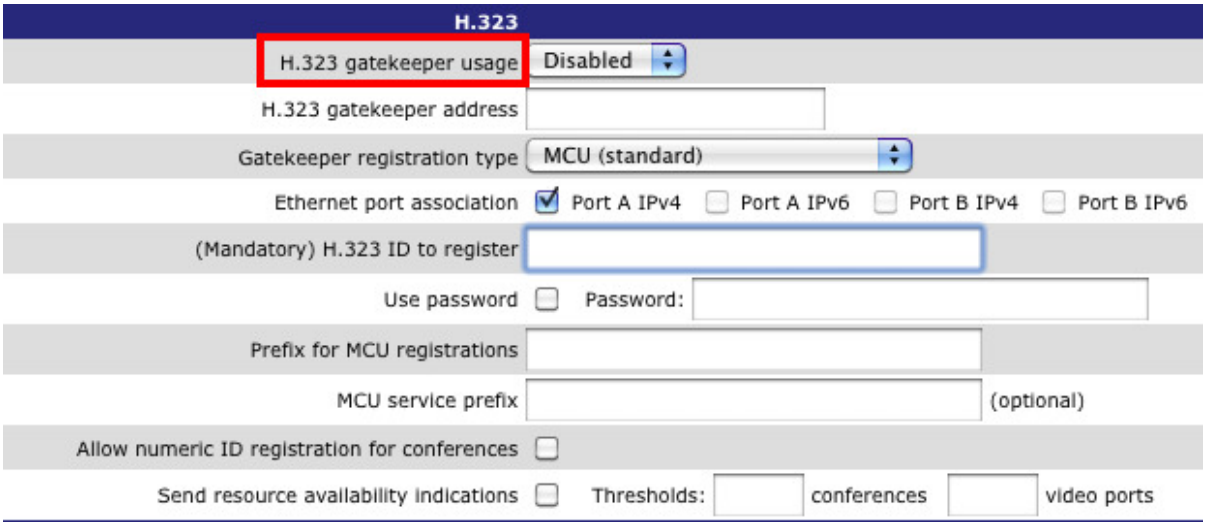
SIP registrar usage	Select *Disabled*. This setting is required for cascading between TelePresence MCUs to be supported.
SIP proxy address	Leave blank. This field must be blank for cascading between TelePresence MCUs to be supported.
Outgoing transport	Select *TLS*.
Use local certificate for outgoing connections and registrations	Check the box.



3. Click **Apply changes**.

Task 5: Disabling H.323 registration

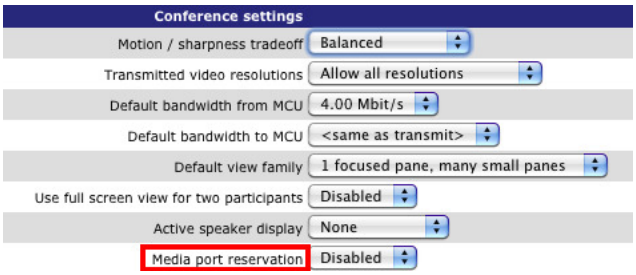
1. Go to **Settings > H.323**.
2. Set **H.323 gatekeeper usage** to *Disabled*.



3. Click **Apply changes**.

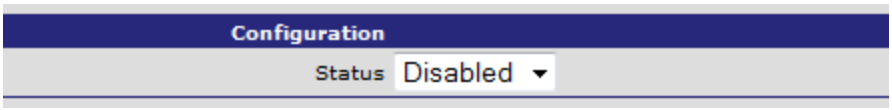
Task 6: Changing miscellaneous settings

1. Go to **Settings > Conferences**.
2. Under Conference Settings ensure **Media port reservation** is set to *Disabled*.



3. Click **Apply changes**.
4. Go to **Gatekeeper > Built in Gatekeeper**.
5. Under **Configuration** ensure **Status** is set to *Disabled*.

   Note: The MCU 5300 series does not have a built-in Gatekeeper.



6. Click **Apply changes**.

Configuring the TelePresence Server

The following tasks are required for both ad hoc and rendezvous conferences when using TelePresence Servers as the conference bridges. You will need to repeat them for all TelePresence Servers in the deployment.

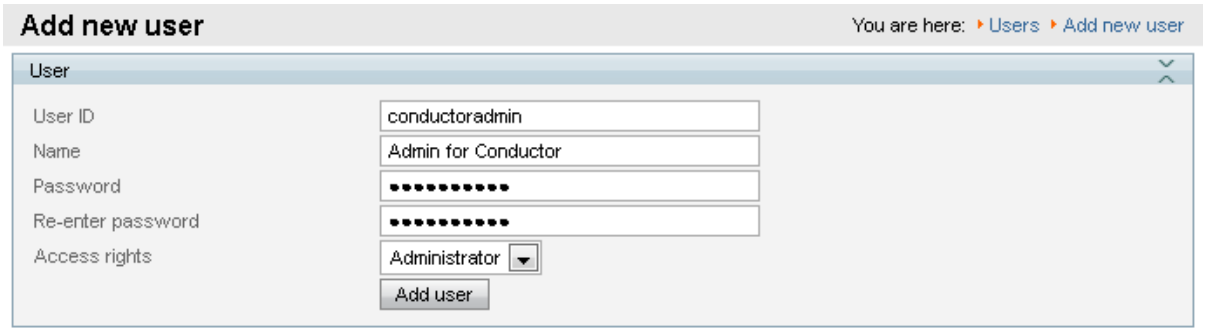
The tasks are not required if only TelePresence MCUs are used in the deployment.

Task 7: Creating a user

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

1. Go to the web interface of the TelePresence Server you want to configure and log in as an administrator.
2. Go to **User > Add New User**.
3. Enter the following in the relevant fields:

User ID	Enter a username for the TelePresence Conductor to use.
Name	Enter a name for this user.
Password	Enter a password for the TelePresence Conductor to use.
Access rights	Select *Administrator*.



4. Click **Add user**.

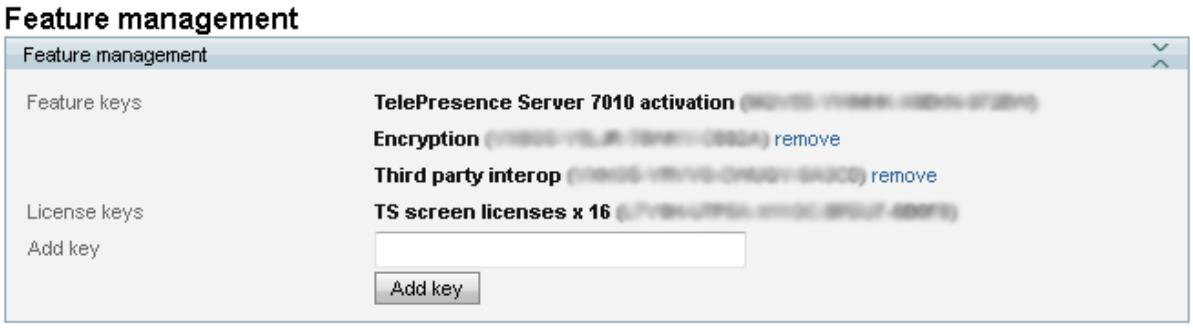
Task 8: Installing an encryption key

The TelePresence Server has the ability to use a secure connection for communications. These security features are enabled with the **Encryption** option key. For TelePresence Server version 4.1(2.33) or earlier, you must install the option key in order for this deployment to work. Beginning with version 4.2, it is no longer required.

Note: The term "Encryption Key" is replaced with "Media Encryption Key" beginning in version 4.2. Most customers outside of Russia will still want to install this key. Encryption keys installed in TelePresence Servers running a software version earlier than 4.2 are automatically converted to media encryption keys when upgrading to version 4.2 or later.

To verify that the *Encryption* key is installed or to install the key, perform the following tasks:

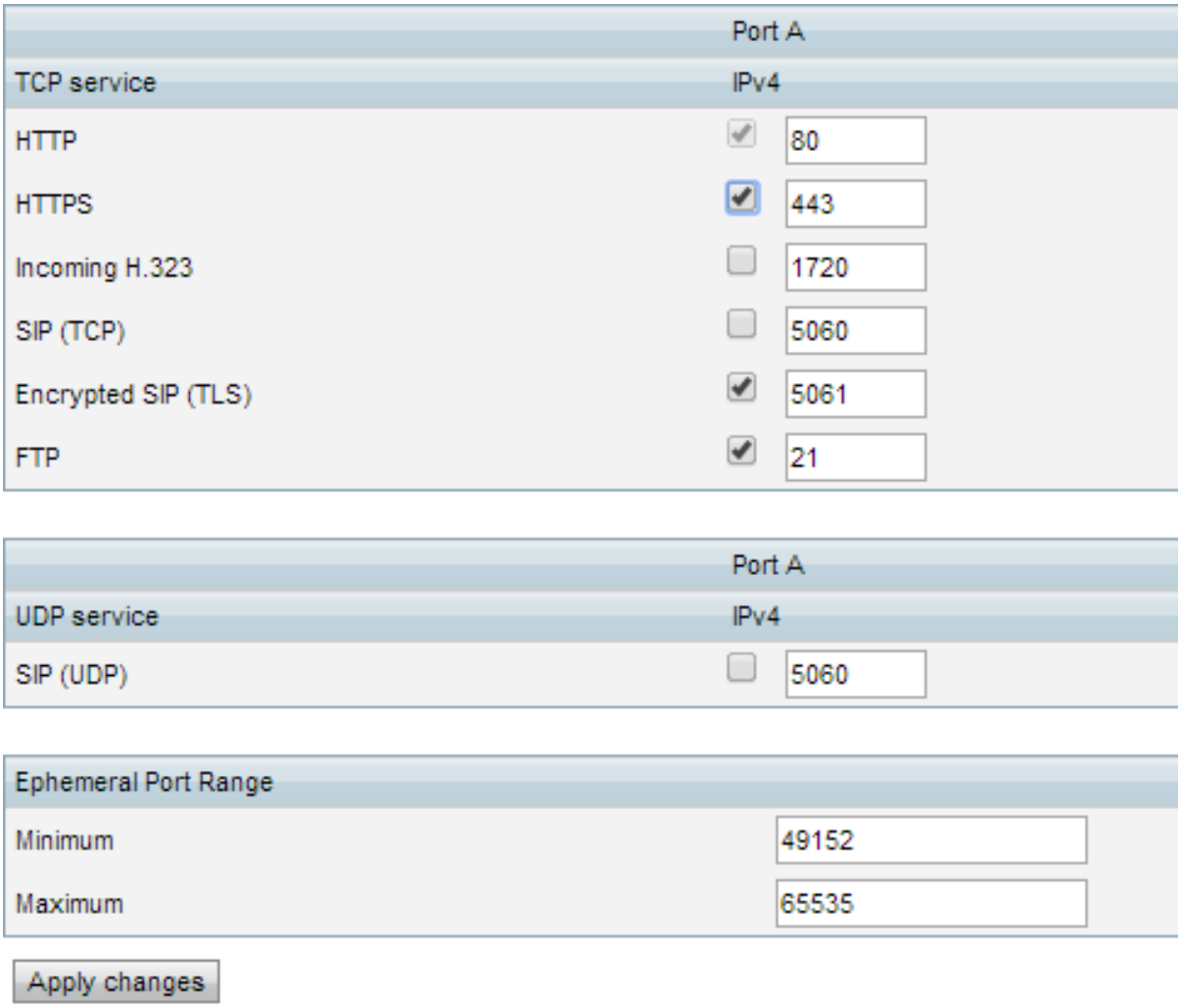
1. Go to **Configuration > Upgrade**.
2. Go to the **Feature management** section and verify that the **Encryption** key is installed. If the key is not installed, enter the key into the **Add key** field and click **Add key**.



To verify that TLS is enabled on the TelePresence Server:

1. Go to **Network > Services**.
2. Ensure that **Encrypted SIP (TLS)** is checked.
3. Ensure that **Incoming H.323**, **SIP (TCP)** and **SIP (UDP)** are not checked.
   H.323 is not available on TelePresence Server on Media 310/320 or Virtual Machine platforms.

4. Ensure that **HTTPS** is enabled on port 443.



5. Click **Apply changes**.

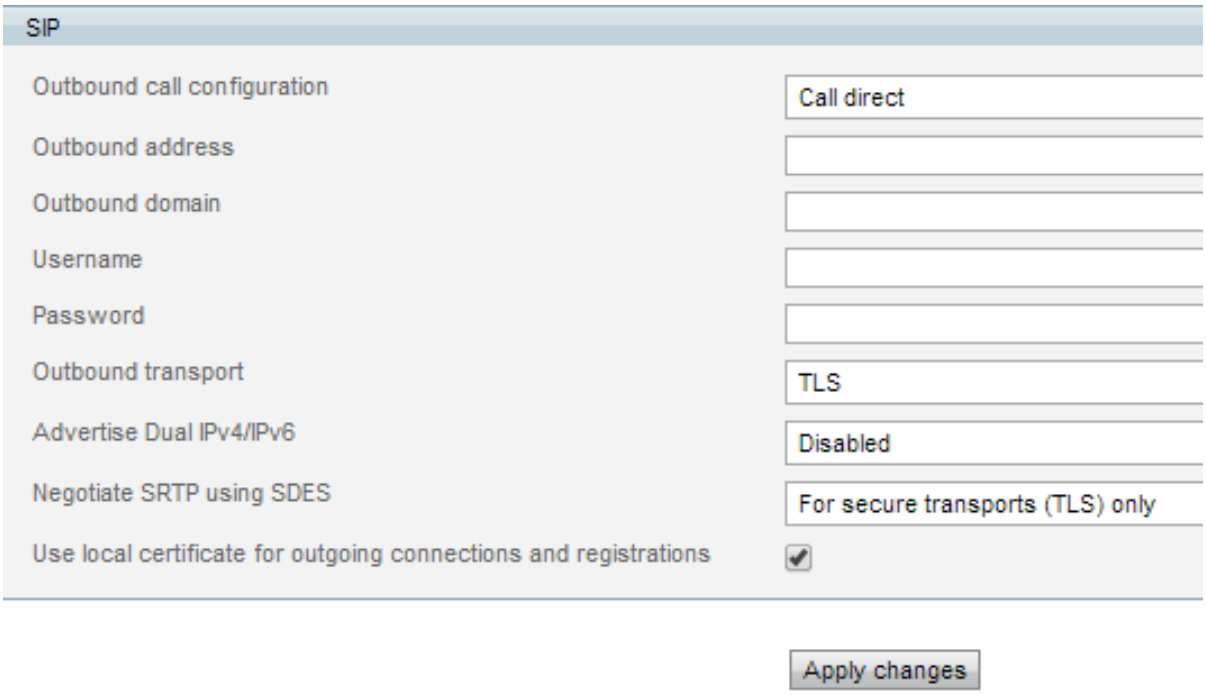
Task 9: Configuring SIP

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

To enable outbound SIP dialing from the TelePresence Server:

1. Go to **Configuration > SIP Settings**.
2. Enter the following values into the relevant fields:

Outbound call configuration	Select *Call direct* from the drop-down list. *Call direct* is required for cascading between TelePresence Servers to be supported.
Outbound address	Leave blank. This field must be left blank for cascading between TelePresence Servers to be supported.
Outbound domain	Leave blank. This field must be left blank for cascading between TelePresence Servers to be supported.
Username	Leave blank.
Password	Leave blank.
Outbound transport	Select *TLS* from the drop-down list.
Advertise Dual IPv4/IPv6	Leave as *Disabled*, unless your deployment uses both IP addressing schemes.
Negotiate SRTP using SDES	Select *For Secure Transport (TLS) only* from the drop-down list.
Use local certificate for outgoing connections and registrations	Check the box. This checkbox is not on all TelePresence Server models: it only appears on the 7010 and MSE 8710 models.



3. Click **Apply changes**.

Task 10: Disabling H.323 registration

Perform the following steps to disable H323 registration to a gatekeeper:

1. Go to **Configuration > H323 Settings**.
2. Uncheck the box for **Use gatekeeper**.
3. Leave all other fields as their default values.
4. Click **Apply changes**.

Task 11: Configuring the operation mode

(This task is not relevant for Cisco TelePresence Server on Virtual Machine or Cisco TelePresence Server on Multiparty Media 310/320. These versions of TelePresence Server always run in *Remotely managed* mode.)

1. Go to **Configuration > Operation mode**.
2. Select *Remotely managed* from the drop down list. This enables the TelePresence Conductor to manage the TelePresence Server.

3. Click **Apply changes**.
4. For the changes to take effect, the TelePresence Server must be restarted. Go to **Configuration > Shutdown**.
5. Click **Shutdown TelePresence Server**.
6. Click **Confirm TelePresence Server shutdown**.
7. Click **Restart TelePresence Server**.
8. After about 3 minutes, the TelePresence Server will be available to the TelePresence Conductor.

Configuring the TelePresence Conductor

This section of the guide assumes that the TelePresence Conductor is reachable over the network. For assistance in reaching this stage please see *Cisco TelePresence Conductor Administrator Guide*.

The following tasks describe the configuration required on TelePresence Conductor. The tasks are split up into:

- general tasks required for both ad hoc and rendezvous conferences
- tasks required for ad hoc conferences only
- tasks for rendezvous conferences only

Configuring general settings on TelePresence Conductor

The following tasks are required when configuring both ad hoc and rendezvous conferences.

Task 12: Changing the administrator password

1. Log into the TelePresence Conductor as the user 'admin' and with the default password 'TANDBERG'.
2. Go to **Users > Administrator accounts**.
3. Click **View/Edit** for the 'admin' user.
4. Enter a new password.
5. Click **Save**.

Note: The TelePresence Conductor will not handle conference requests if it has the administrator password set to its default value.

Task 13: Changing the root password

1. Log in to the TelePresence Conductor as root (default password = 'TANDBERG'). By default you can only do this using SSH or a serial connection.
2. Type **`passwd`**.
3. Enter the new password, and when prompted, retype the new password.
4. You will receive the message:
   `passwd: password updated successfully`
5. Type 'exit' to log out of the root account.

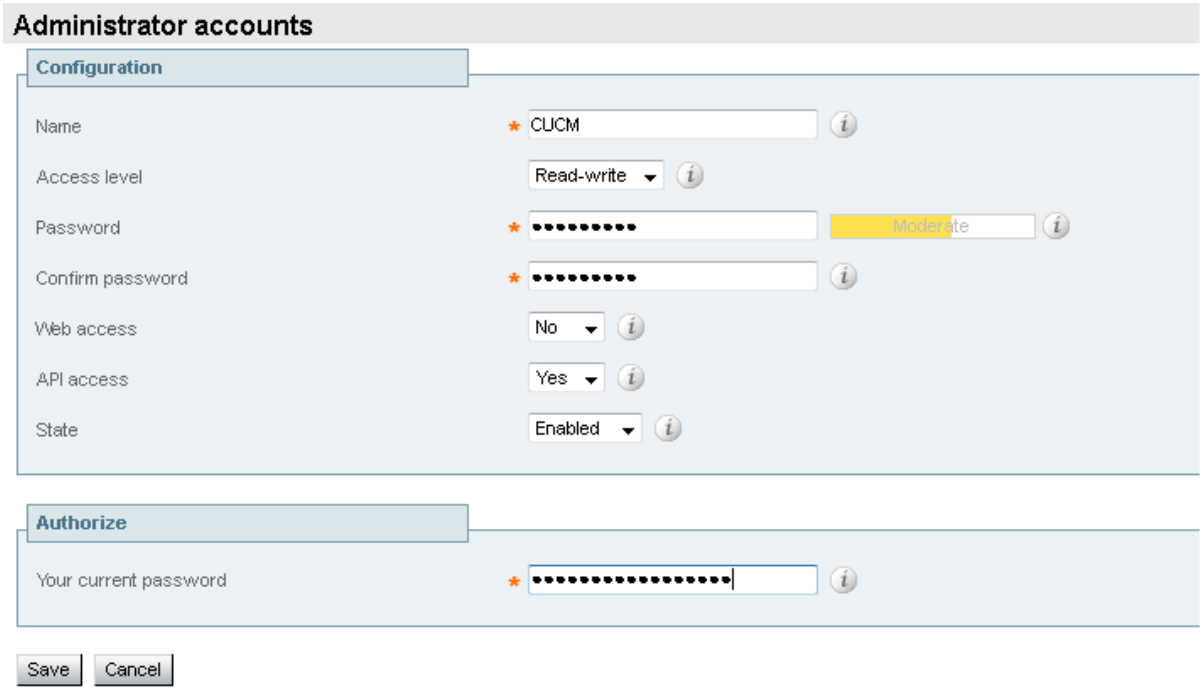
Note: The TelePresence Conductor will not handle conference requests if it has the root password set to its default value.

Task 14: Creating a user for Unified CM access

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

1. Log into the TelePresence Conductor as a user with administrator rights.
2. Go to **Users > Administrator accounts**.
3. Click **New**.
4. Enter the following in the relevant fields:

Name	Enter a name for this user.
Access level	Select *Read-write*.
Password	Enter a password for this account.
Confirm password	Re-enter the same password.
Web access	This does not need to be enabled, except to verify the account credentials are correct in a troubleshooting scenario. Select *No*.
API access	Select *Yes*.
State	Select *Enabled*.
Your current password	Enter the password that you are currently logged in with to authorize the change.

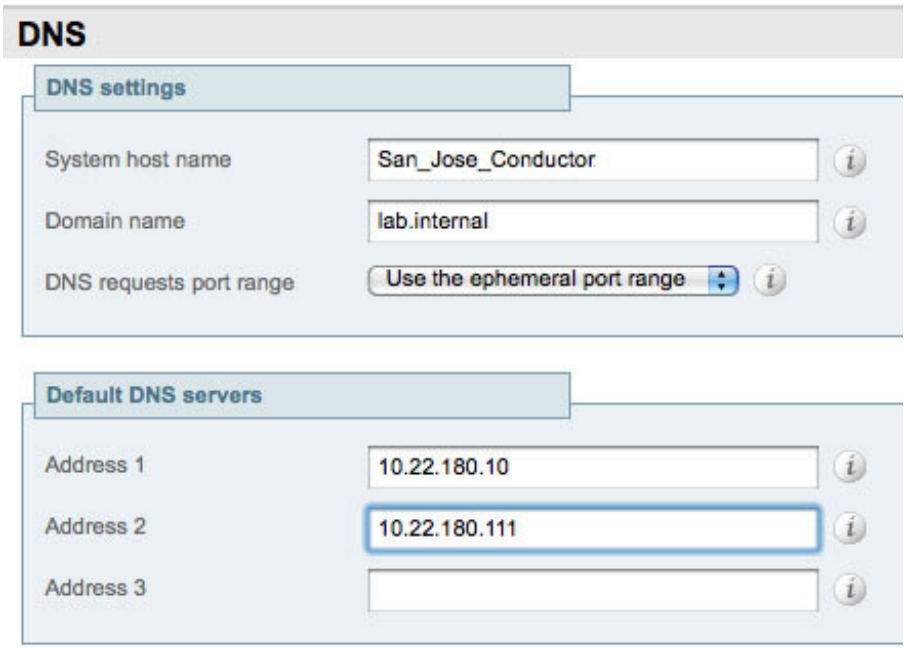


5. Click **Save**.

Task 15: Changing the system settings

1. Go to **System > DNS**.
2. Enter the following values into the relevant fields:

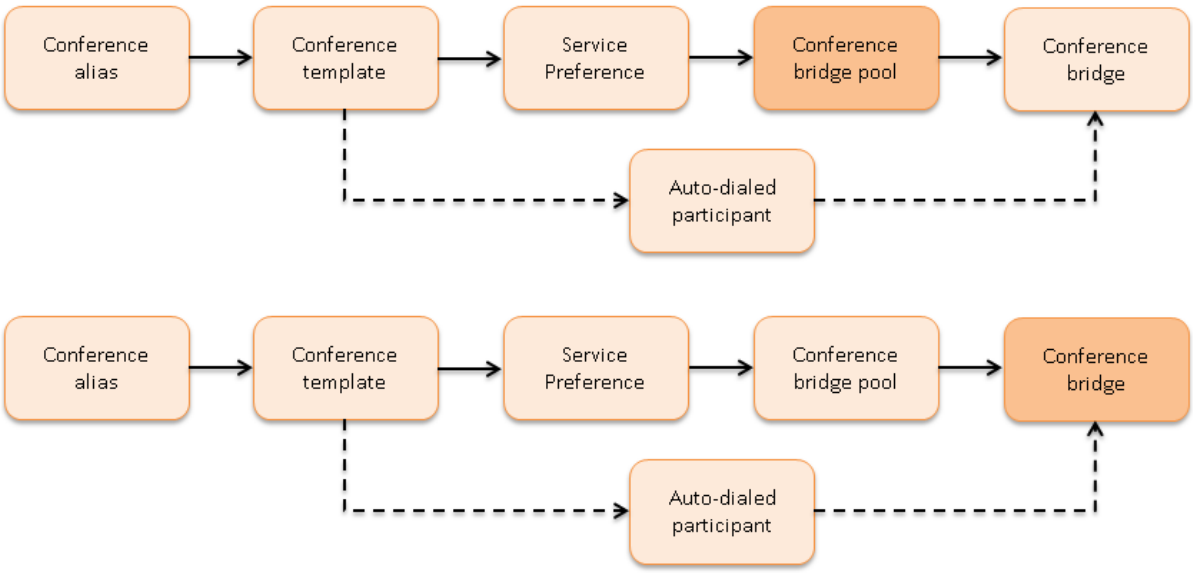
System host name	Enter the hostname of your TelePresence Conductor.
Domain name	Enter the domain for your TelePresence Conductor.
Address 1	Enter the IP address of the DNS server.
Address 2	Enter the IP address of your backup DNS server.



Note: the FQDN of the TelePresence Conductor will be <System host name>.<Domain name>

3. Click **Save**.
4. Go to **System > Time**. If the default servers are unreachable then it may be necessary to enter alternate NTP servers.
5. Ensure that under the **Status** section the **State** is *Synchronized*. This can take a couple of minutes.

Task 16: Setting up conference bridge pools



To set up a conference bridge pool, you need to create a conference bridge pool and then add one or more conference bridge(s) to it. The following examples show how to set up conference bridge pools for:

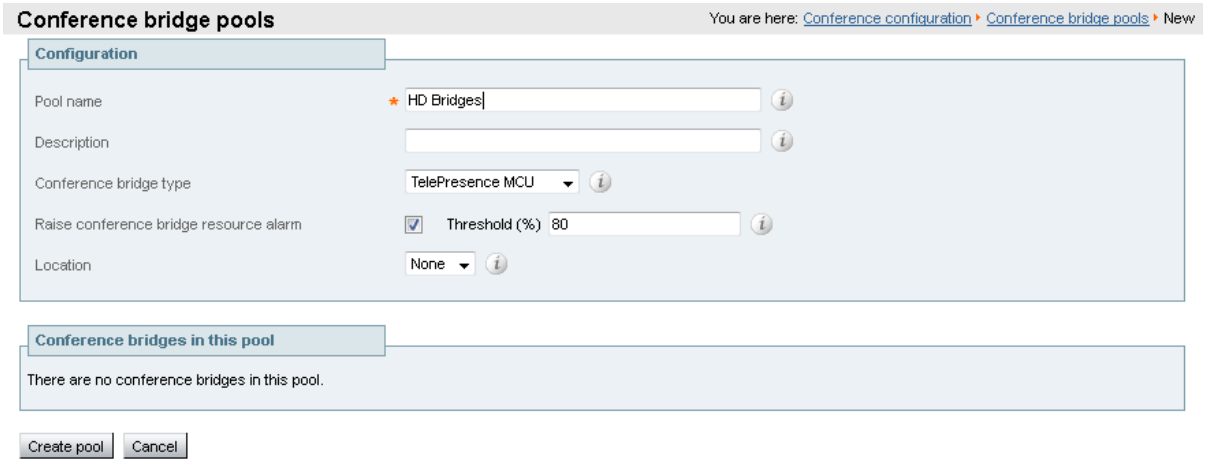
- TelePresence MCU hosted conferences
- TelePresence Server hosted conferences

Note: We strongly recommend that all conference bridges within a pool have the same capacity, so that conferences can be distributed efficiently across conference bridges. If there are conference bridges with different capacities in the same pool, this may lead to unbalanced conference placement in some scenarios.

Creating a TelePresence MCU conference bridge pool

1. Go to **Conference configuration > Conference bridge pools**.
2. Click **New**.
3. Enter the following values into the relevant fields:

Pool name	Enter a name for the conference bridge pool.
Conference bridge type	Select the appropriate bridge type, *TelePresence MCU*.
Location	Select *None* for now. You will go back to select a **Location** in a later step, after the **Location** has been added.



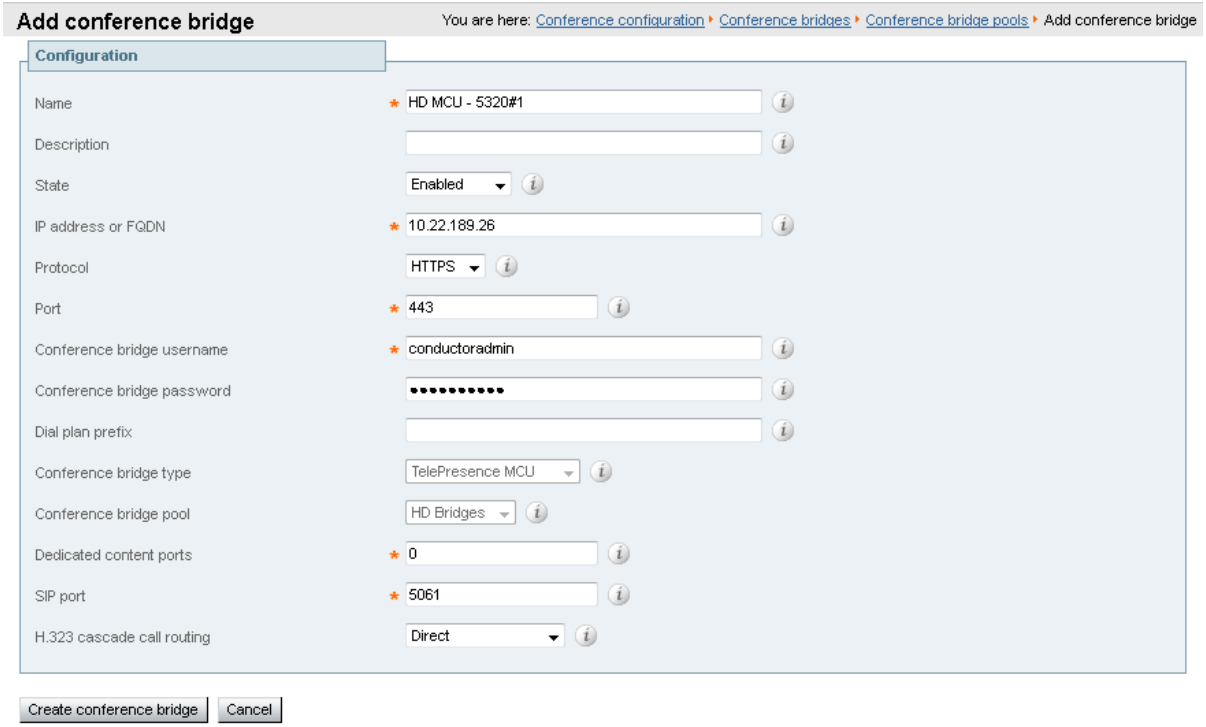
4. Click **Create pool**.

Adding a conference bridge to the TelePresence MCU conference bridge pool

1. From the **Conference bridge pools** page click **Create conference bridge**.
2. Enter the following values into the relevant fields:

Name	Enter a name for the conference bridge.

State	Select *Enabled*.
IP address or FQDN	Enter the IP address of the conference bridge.
Protocol	Select *HTTPS*.
Port	Enter '443'.
Conference bridge username	Enter the conference bridge admin username (created in Task 2: Creating a user [p.15]).
Conference bridge Password	Enter the conference bridge password for this user.
Dial plan prefix	Leave this blank.
Dedicated content ports	Enter the appropriate value for your TelePresence MCU. To discover if a TelePresence MCU has any dedicated content ports follow the steps given in Appendix 7: Identifying dedicated content ports on a Cisco TelePresence MCU [p.102].
SIP port	Enter the SIP Port on which the TelePresence MCU is to listen for SIP TLS traffic; typically this is '5061'.
H.323 cascade call routing	Select *Direct*. **Note:** this field only affects calls from one TelePresence MCU to another for cascade links.



3. Click **Create conference bridge**.
4. Ensure that under the **Conference bridges in this pool** section, under the **Status** header the conference bridge is listed as *Active*.

5. Repeat the steps to add any further TelePresence MCUs to the conference bridge pool.

Configuring a TelePresence Server conference bridge pool

1. Go to **Conference configuration > Conference bridge pools**.
2. Click **New**.
3. Enter the following values into the relevant fields:

Pool name	Enter a name for the conference bridge pool.
Conference bridge type	Select the appropriate bridge type, *TelePresence Server*.
Location	Select *None* for now. You will go back to select a **Location** in a later step, after the **Location** has been added.

4. Click **Create pool**.

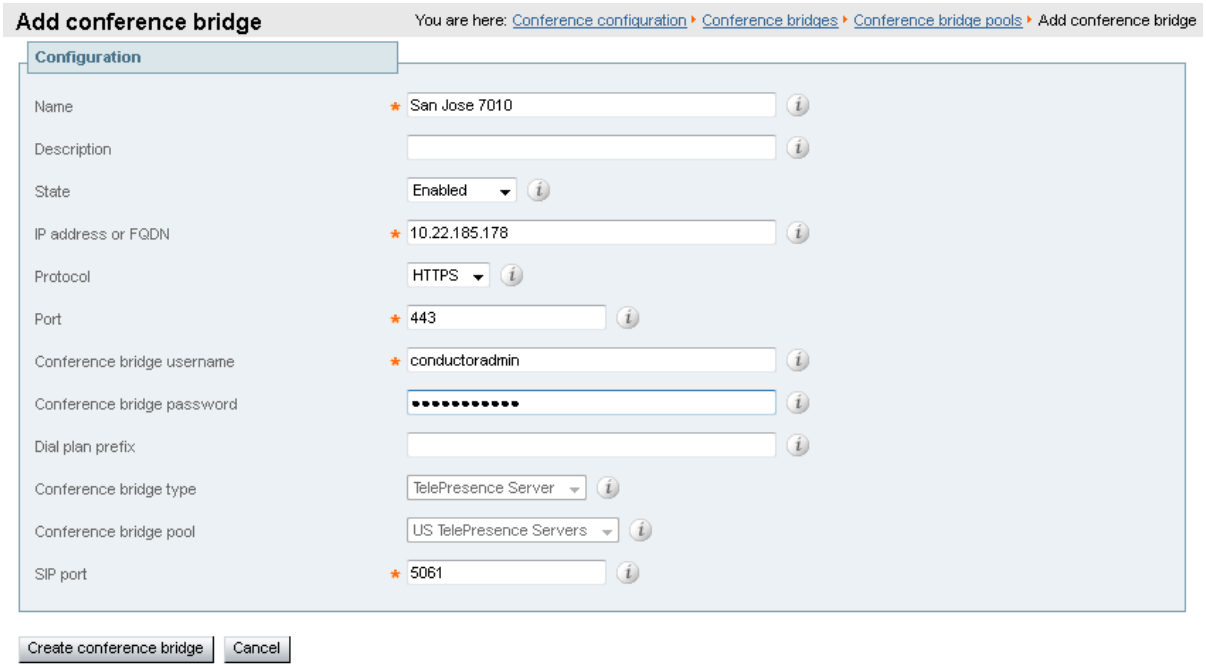
Adding a conference bridge to the TelePresence Server conference bridge pool

Before adding a TelePresence Server to the conference bridge pool, ensure that the **Operation mode** on the TelePresence Server is set to *Remotely managed* (see Task 11: Configuring the operation mode [p.24]).

1. From the **Conference bridge pools** page click **Create conference bridge**.
2. Enter the following values into the relevant fields:

Name	Enter a name for the conference bridge.
State	Select *Enabled*.
IP address or FQDN	Enter the IP address of the conference bridge.
Protocol	Select *HTTPS*.
Port	Enter '443'.
Conference bridge username	Enter the conference bridge admin username (created in Task 7: Creating a user [p.20]).
Conference bridge password	Enter the conference bridge password for this user.

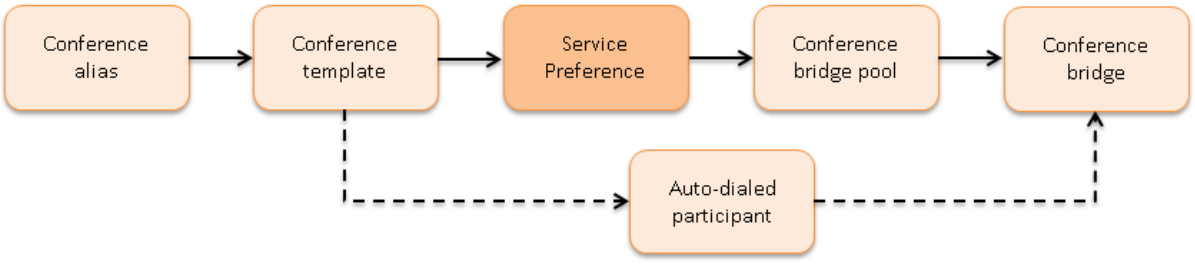
Dial plan prefix	This must be left blank.
SIP port	Enter the SIP port on which the TelePresence Server is to listen for SIP TLS traffic, typically this is '5061'.



3. Click **Create conference bridge**.
4. Ensure that under the **Conference bridges in this pool** section, under the **Status** header the conference bridge is listed as *Active*.

5. Repeat the steps to add any further TelePresence Servers to the conference bridge pool.

Task 17: Creating Service Preferences



A Service Preference is a prioritized list of conference bridge pools that defines the order in which resources are used for conferences. During the configuration process, the conference bridge type is chosen as either

TelePresence MCU or *TelePresence Server*. There is not an ability to mix the different types of conference bridges. A conference can be cascaded from one conference bridge to another, taking into account the prioritized list of conference bridge pools.

The following examples show how to create Service Presences for:

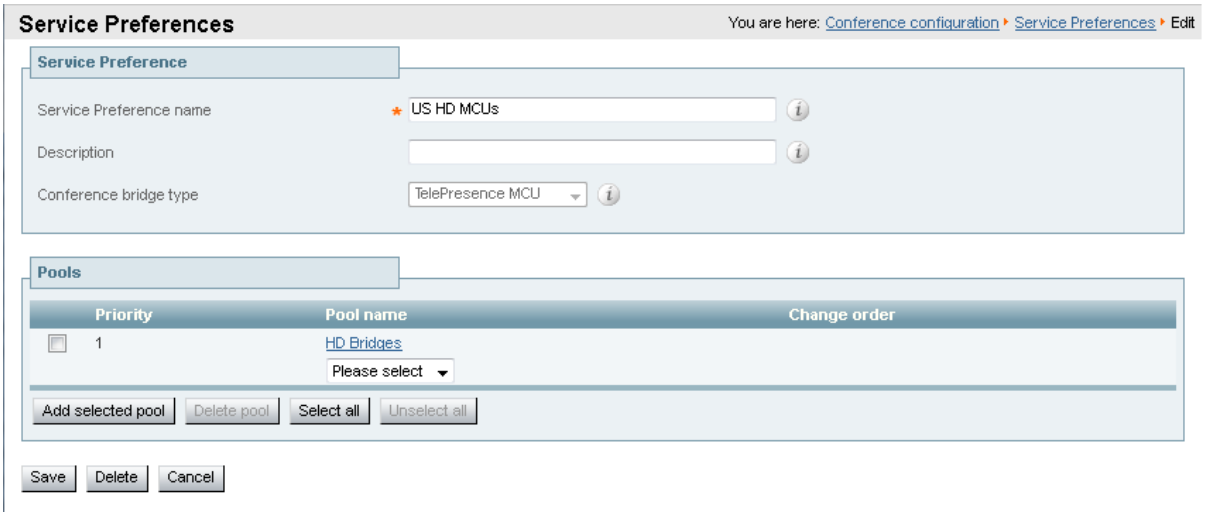
- TelePresence MCU hosted conferences
- TelePresence Server hosted conferences

Creating a Service Preference for TelePresence MCU hosted conferences

1. Go to **Conference configuration > Service Preferences**.
2. Click **New**.
3. Enter the following values into the relevant fields:

Service Preference name	Enter the name of the Service Preference.
Conference bridge type	Select *TelePresence MCU*.

4. Click **Add Service Preference**.
5. In the **Pools** section under **Pool name** select the conference bridge pool containing the TelePresence MCUs.



6. Click **Add selected pool**.
7. Click **Save**.

Creating a Service Preference for TelePresence Server hosted conferences

1. Go to **Conference configuration > Service Preferences**.
2. Click **New**.

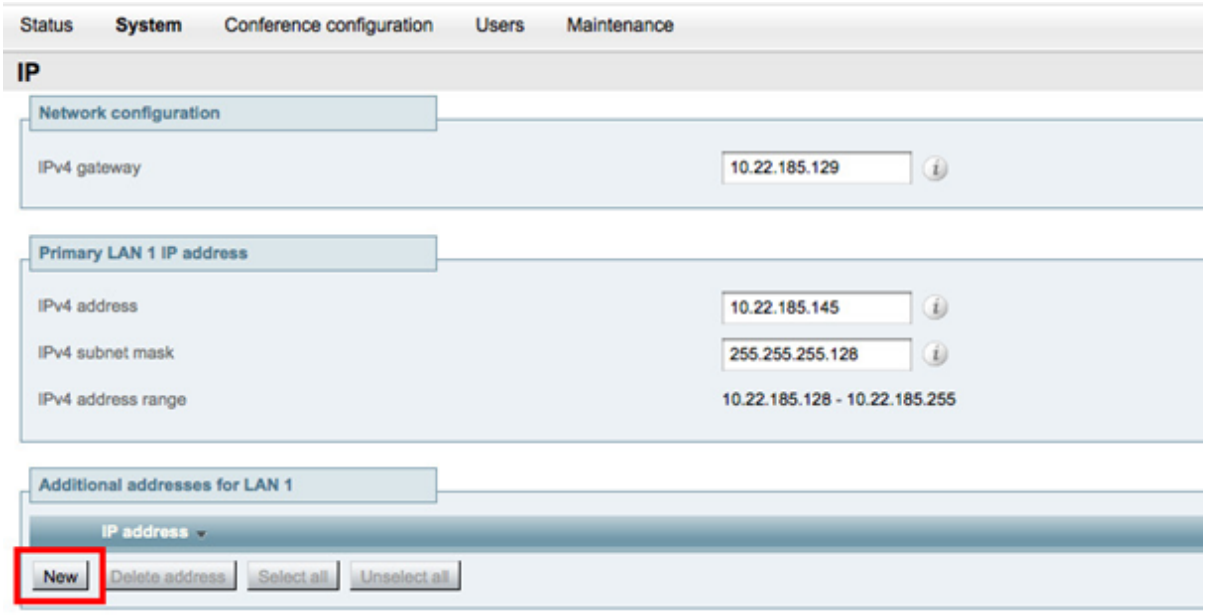
3. Enter the following values into the relevant fields:

Service Preference name	Enter the name of the Service Preference.
Conference bridge type	Select *TelePresence Server*.

4. Click **Add Service Preference**.
5. In the **Pools** section under **Pool name** select the conference bridge pool containing the TelePresence Servers.
6. Click **Add selected pool**.
7. Click **Save**.

Task 18: Adding IP addresses for ad hoc and rendezvous locations on TelePresence Conductor

1. Go to **System > Network interfaces > IP**.
2. In the **Additional addresses for LAN 1** section click **New**.



3. Enter the new **IP address** to be used.

   Note: the IP address must be on the same subnet as the primary TelePresence Conductor IP interface, and must be reserved for use by this TelePresence Conductor alone.

4. Click **Add address**.

5. Repeat steps 2 through 4 until you have added IP addresses for ad hoc and/or rendezvous handling for each Location to be supported.
6. In the **Additional addresses for LAN 1** list, verify that the IP addresses were added correctly.
7. Go to **Maintenance > Restart options**.
8. Click **Restart** to apply network interface changes.
9. Wait for the TelePresence Conductor to restart.
10. To verify the new TelePresence Conductor IP address is active on the network, ping the IP address from another device.

Task 19: Adding FQDNs to server certificate

To allow the TelePresence Conductor to establish an HTTPS connection to the Unified CM, you must add the TelePresence Conductor's fully FQDNs (fully qualified domain names - configured in Task 18: Adding IP addresses for ad hoc and rendezvous locations on TelePresence Conductor [p.35]) to the server certificate's SAN (subject alternative name) list. To do this:

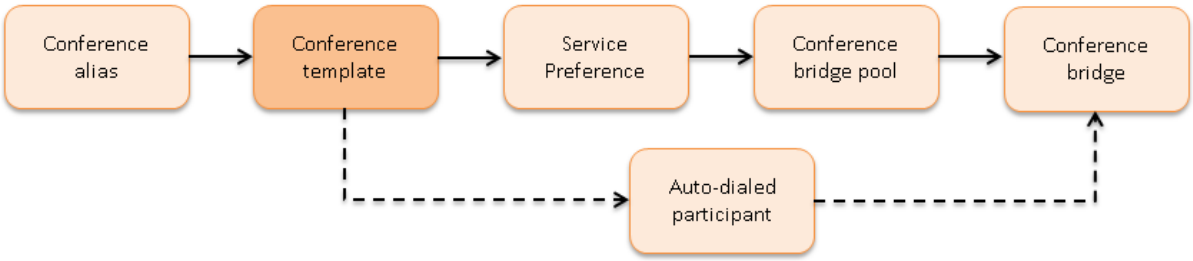
1. Go to **Maintenance > Security certificates > Server certificate**.
2. Under **Certificate signing request (CSR)** click on **Generate CSR**.
3. Under **Alternative name** enter the FQDN into the field **Additional alternative names**. If there is more than one FQDN configured on the TelePresence Conductor, enter all FQDNs, separated by comma.
4. Under **Additional information** enter the appropriate information.
5. Click **Generate CSR**.

If you do not need an HTTPS connection or if you are using a private CA (certificate authority) see Appendix.

Configuring TelePresence Conductor for ad hoc conferences

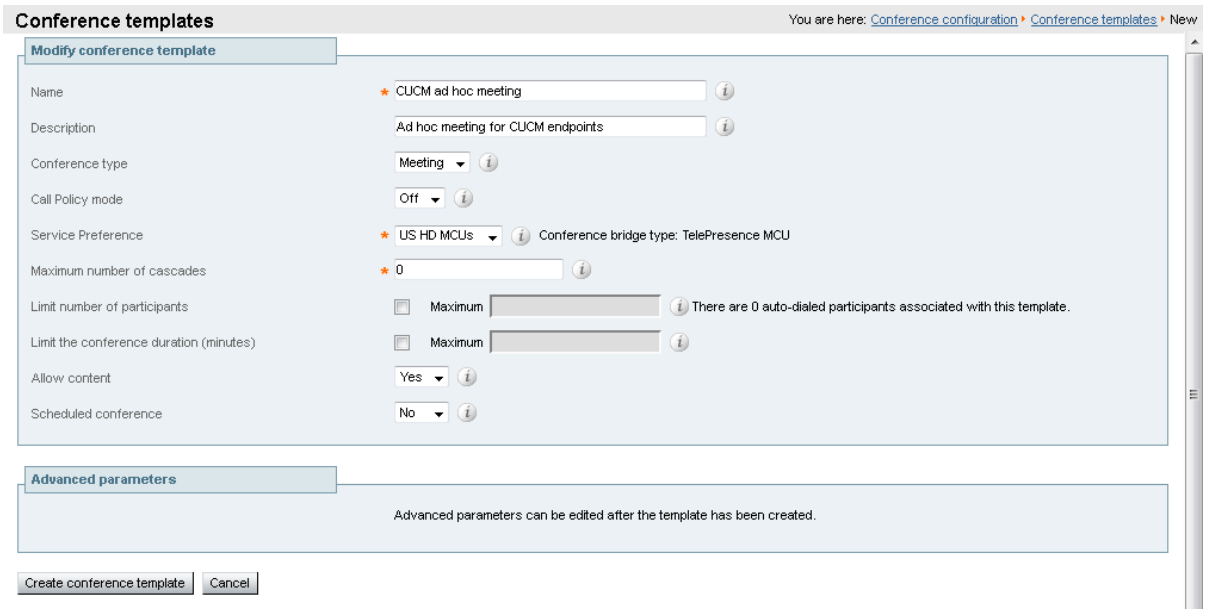
The following tasks are required when configuring ad hoc conferences.

Task 20: Creating a conference template for an ad hoc Meeting-type conference



1. Go to **Conference configuration > Conference templates**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the conference template.
Conference type	Select *Meeting*.
Service Preference	Select the appropriate Service Preference for this template. The type of bridges used (TelePresence Server or TelePresence MCU) will be defined by the Service Preference selected.
Maximum number of cascades	Enter '0' to disable cascade resource reservation. This is required because cascading is not supported for ad hoc conferences.
Participant quality	(Only available if the Service Preference selected is for TelePresence Servers) Select the desired quality for all participants joining the conference. When using a CTS3000 or TX9000 you must select *Full HD (1080p 30fps / 720p 60fps video, multi-channel audio)* or a custom quality setting that has an audio quality level of multi-channel, otherwise insufficient resources will be allocated to display multiple screens.



4. Configure other entries as required.
5. Click **Create conference template**.

Note: If you would like to make changes to the advanced template parameters, which change settings on the conference bridges, see the section *Adding and editing advanced template parameters* within the current *Cisco TelePresence Conductor Administrator Guide*.

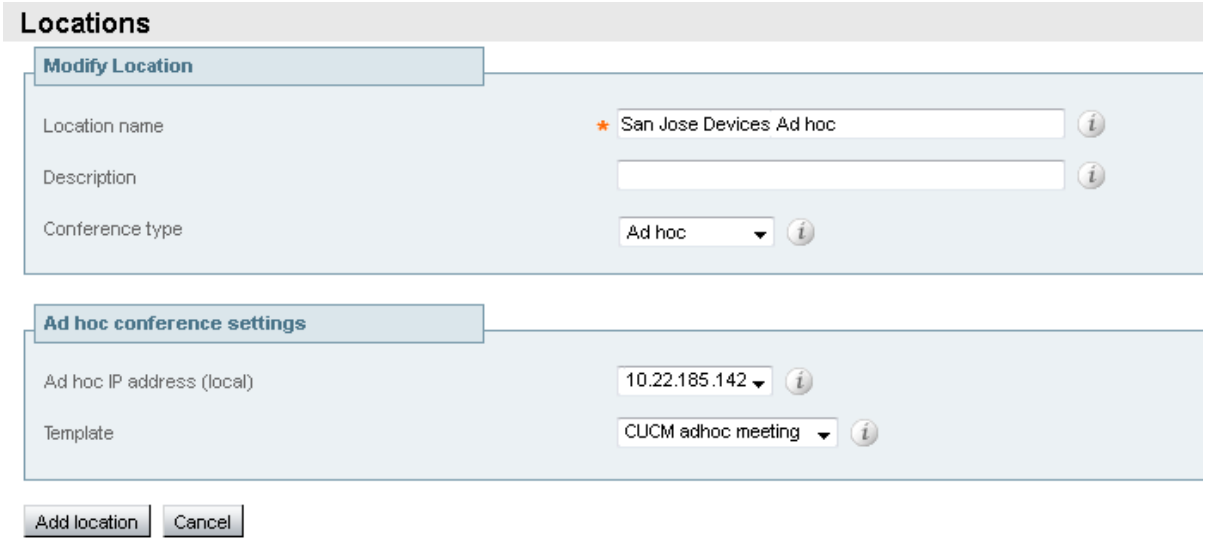
Note: if an ad hoc conference template has been configured to challenge participants for a PIN (via the **Advanced parameters**) participants will be prompted for the PIN when the ad hoc conference is created. Pre-configured endpoints in TelePresence Conductor that have the **Bypass conference PIN entry** field set to *Bypass PIN entry* are not challenged for a PIN even if the conference template has a PIN defined.

Task 21: Creating an ad hoc Location

1. Go to **Conference configuration > Locations**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Location name	Enter a name.
Conference type	Select *Ad hoc* or *Both*, from the drop-down list. In this example *Ad hoc* was selected.
Ad hoc IP address	From the drop down list, select the TelePresence Conductor IP address to be used for ad hoc calls in this location. This will be the value configured as the **Destination address** of the Conference Bridge configured on Unified CM

Ad hoc template	Select a template from the drop-down list – ensure that this template uses a Service Preference which only contains pools of conference bridges situated in this location.

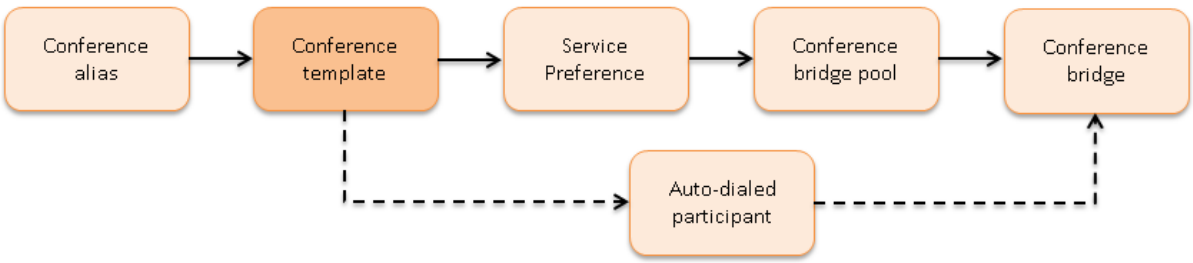


4. Click **Add location**.

Configuring TelePresence Conductor for rendezvous conferences

The following tasks are required when configuring rendezvous conferences.

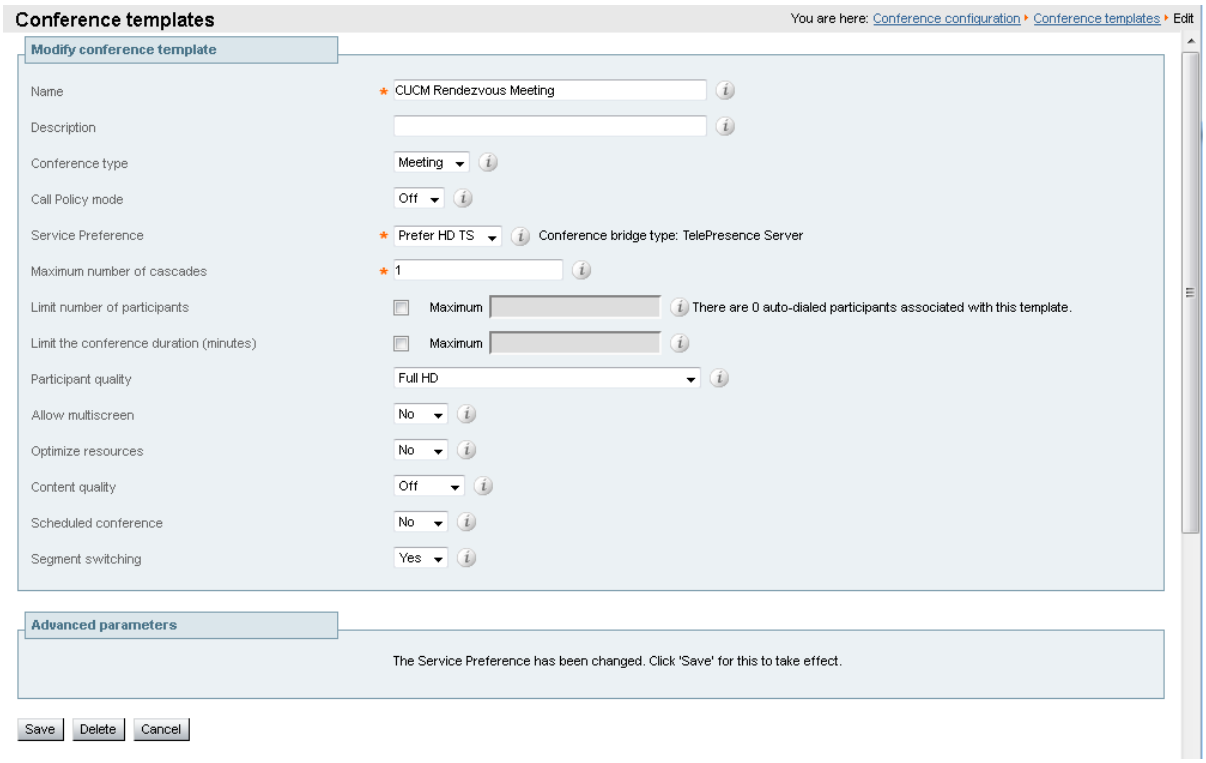
Task 22: Creating a conference template for a rendezvous Meeting-type conference



1. Go to **Conference configuration > Conference templates**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the conference template.

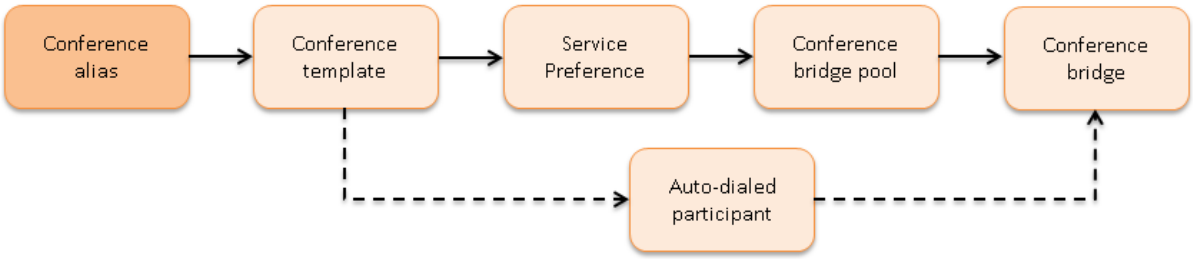
Conference type	Select *Meeting* (a Lecture-type conference can also be configured - that would require two aliases to be configured, a 'Guest' alias and a 'Host' alias).
Service Preference	Select the appropriate Service Preference for this template. The type of bridges used (TelePresence Server or TelePresence MCU) will be defined by the Service Preference selected.
Maximum number of cascades	To enable cascading, enter 1 (the default), or a higher number if you want to cascade to more than one conference bridge. To disable cascading, enter '0'.
Limit number of participants	Specify a limited number of participants, if required. The number includes any auto-dialed participants and any reserved hosts (if Lecture was specified). **Note:** No preference is given to participants who have organized a conference. If the maximum number of participants is reached before the participant who organized the conference has dialed in, this participant is rejected.
Participant quality	(Only available if the Service Preference selected is for TelePresence Servers) Select the desired quality for all participants joining the conference. When using a CTS3000 or TX9000 you must select *Full HD (1080p 30fps / 720p 60fps video, multi-channel audio)* or a custom quality setting that has an audio quality level of multi-channel, otherwise insufficient resources will be allocated to display multiple screens.



4. Configure other entries as required.
5. Click **Create conference template**.

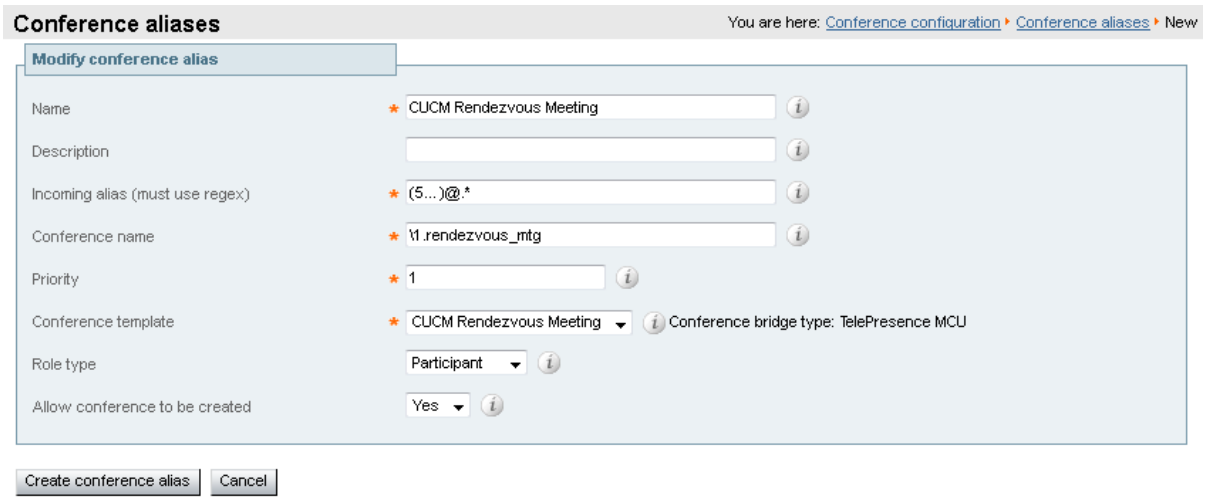
Note: If you would like to make changes to the advanced template parameters, which change settings on the conference bridges, see the section *Adding and editing advanced template parameters* within the current *Cisco TelePresence Conductor Administrator Guide*.

Task 23: Creating a conference alias for a rendezvous Meeting-type conference



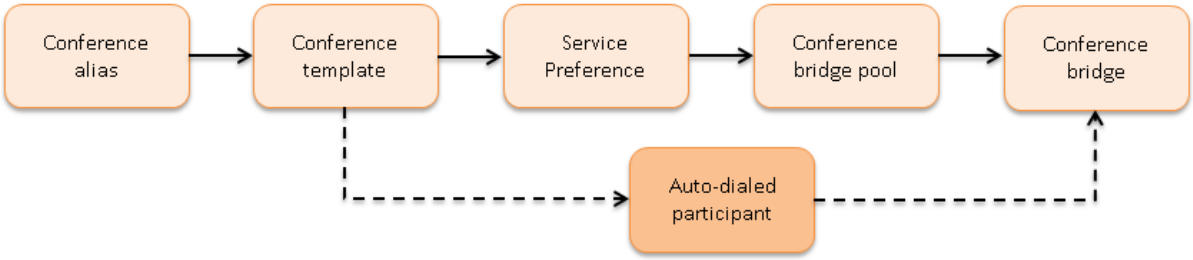
1. Go to **Conference configuration > Conference aliases**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the conference alias.
Incoming alias	Enter the regex expression to match the incoming string from Unified CM, for example `(5…)@.*` or a more specific pattern. Note that SIP requests received from Unified CM are in the format `name@<IP address | FQDN>:<port>`.
Conference name	Enter a regular expression or create the name of the conference to which this participant will be added.
Priority	Enter the priority for this alias.
Conference template	Select the appropriate template.
Role type	Select *Participant*.



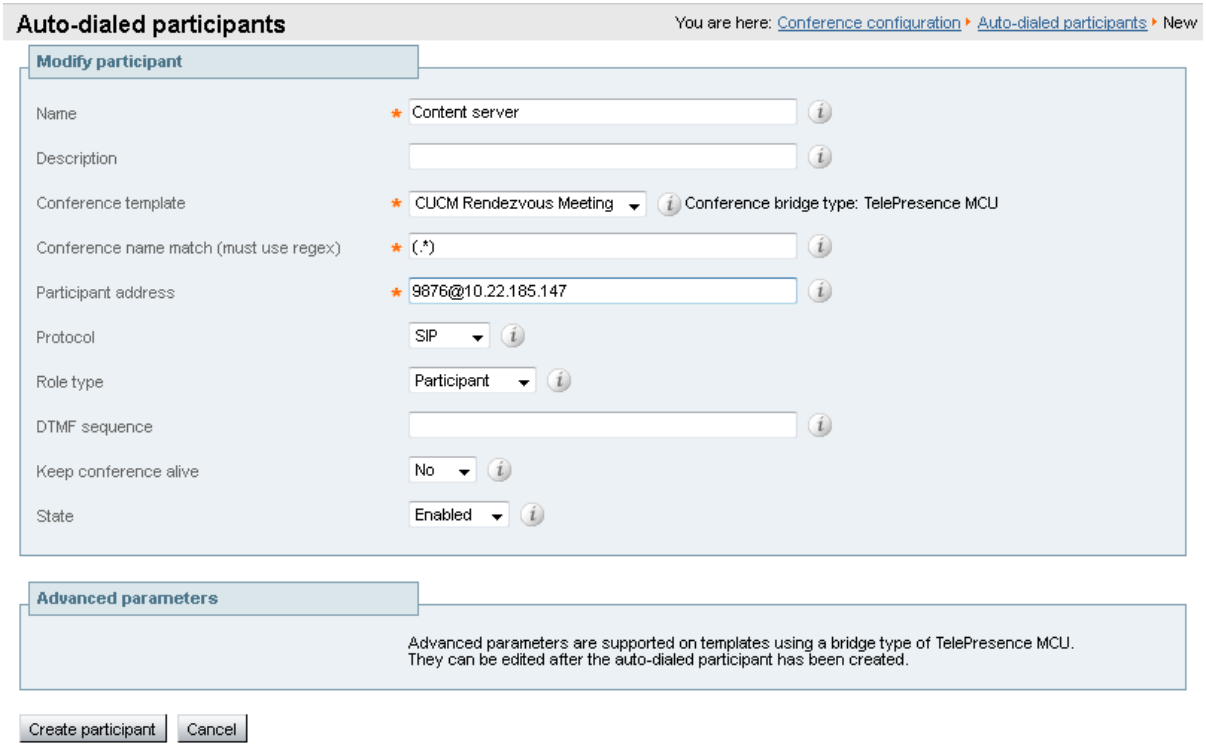
4. Click **Create conference alias**.

Task 24: Creating an auto-dialed participant for a rendezvous Meeting-type conference



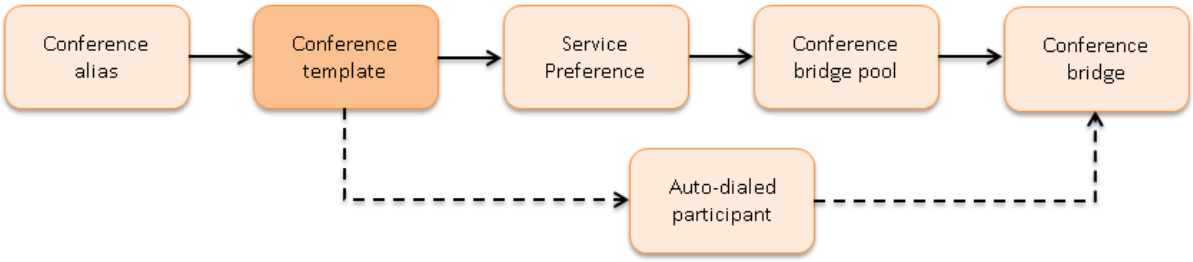
1. Go to **Conference configuration > Auto-dialed participants**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the auto-dialed participant.
Conference template	Select the appropriate template.
Conference name match	Enter the regular expression or specific conference name that matches the name of the conference to which this participant will be added.
Participant address	Enter the dial string to reach this participant. This needs to contain the Unified CM IP address or a domain.
Protocol	Select *SIP*.
Role type	Select *Participant*.
State	Select *Enabled*.



4. Click **Create participant**.

Task 25: Creating a conference template for a rendezvous Lecture-type conference

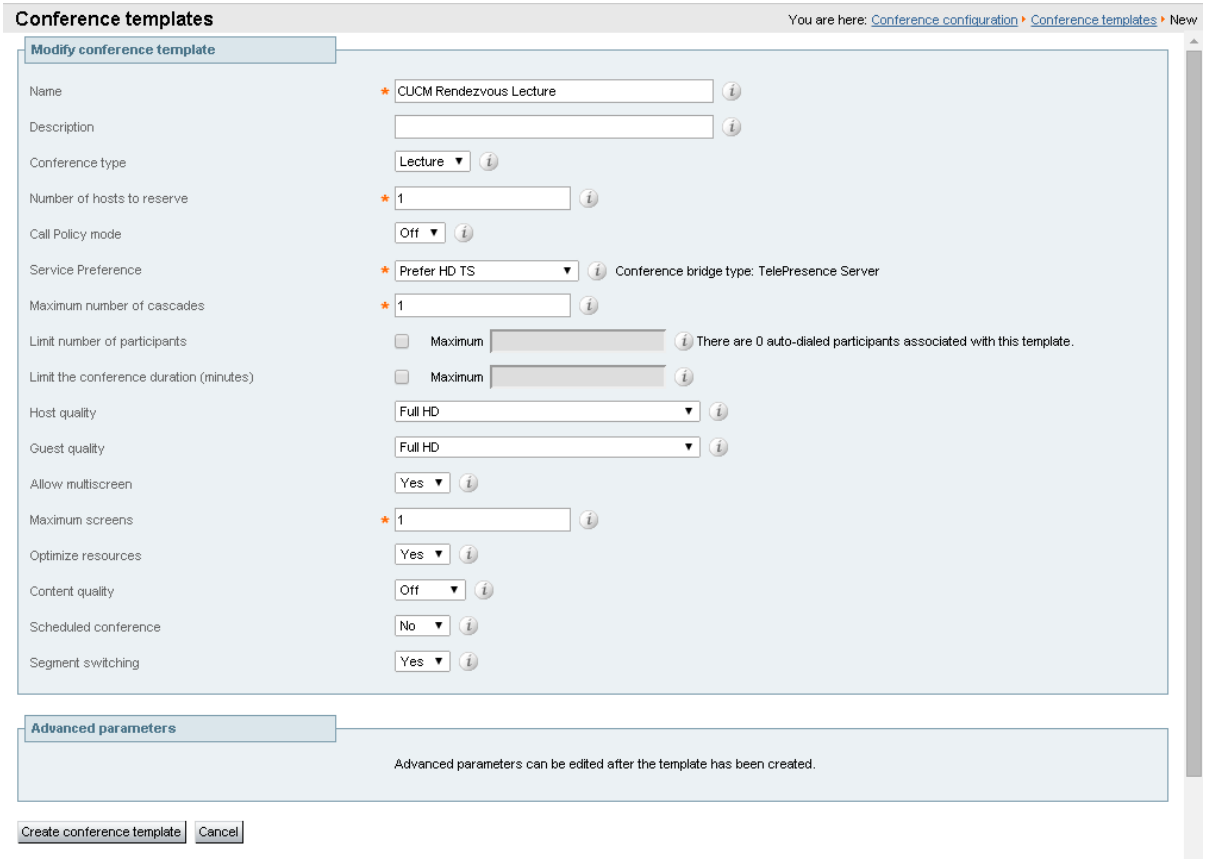


Note: When configuring conference aliases for 'Lecture'-type conferences, you must ensure that the **Conference name** for the 'Host' alias and the 'Guest' alias resolve to the same string. If you do not, they will end up in separate conferences.

1. Go to **Conference configuration > Conference templates**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the conference template.

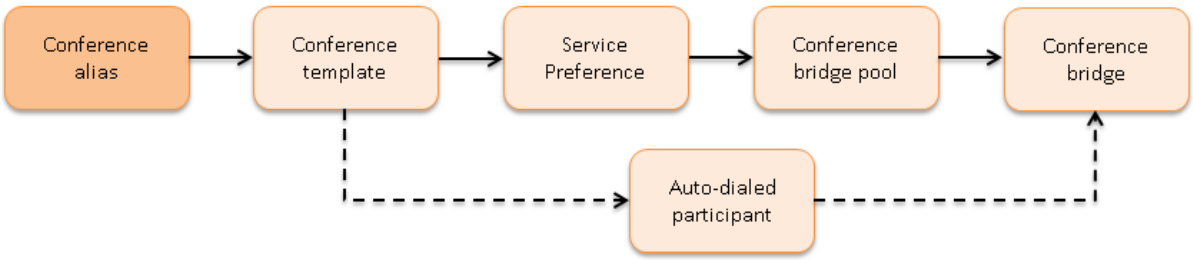
Conference type	Select *Lecture*.
Number of hosts to reserve	Specify the number of hosts to reserve resources for.
Service Preference	Select the appropriate Service Preference for this template. The type of bridges used (TelePresence Server or TelePresence MCU) will be defined by the Service Preference selected.
Maximum number of cascades	To enable cascading, enter 1 (the default), or a higher number if you want to cascade to more than one conference bridge. To disable cascading, enter '0'.
Limit number of participants	Specify a limited number of participants, if required. The number includes any auto-dialed participants and any reserved hosts (if Lecture was specified). **Note:** No preference is given to participants who have organized a conference. If the maximum number of participants is reached before the participant who organized the conference has dialed in, this participant is rejected.
Host quality	(Only available if the Service Preference selected is for TelePresence Servers) Select the desired quality for all hosts joining the conference. When using a CTS3000 or TX9000 you must select *Full HD (1080p 30fps / 720p 60fps video, multi-channel audio)* or a custom quality setting that has an audio quality level of multi-channel, otherwise insufficient resources will be allocated to display multiple screens.
Guest quality	(Only available if the Service Preference selected is for TelePresence Servers) Select the desired quality for all guests joining the conference. When using a CTS3000 or TX9000 you must select *Full HD (1080p 30fps / 720p 60fps video, multi-channel audio)* or a custom quality setting that has an audio quality level of multi-channel, otherwise insufficient resources will be allocated to display multiple screens.



4. Configure other entries as required.
5. Click **Create conference template**.

Note: If you would like to make changes to the advanced template parameters, which change settings on the conference bridges, see the section *Adding and editing advanced template parameters* within the current *Cisco TelePresence Conductor Administrator Guide*.

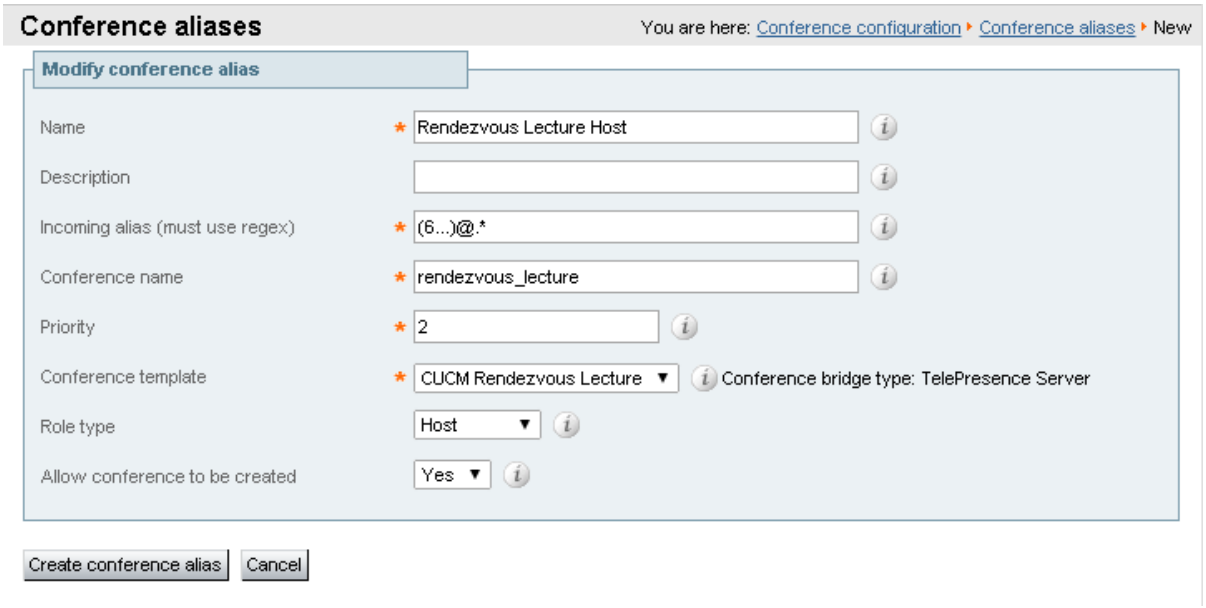
Task 26: Creating a host conference alias for a rendezvous Lecture-type conference



1. Go to **Conference configuration > Conference aliases**.
2. Click **New**.

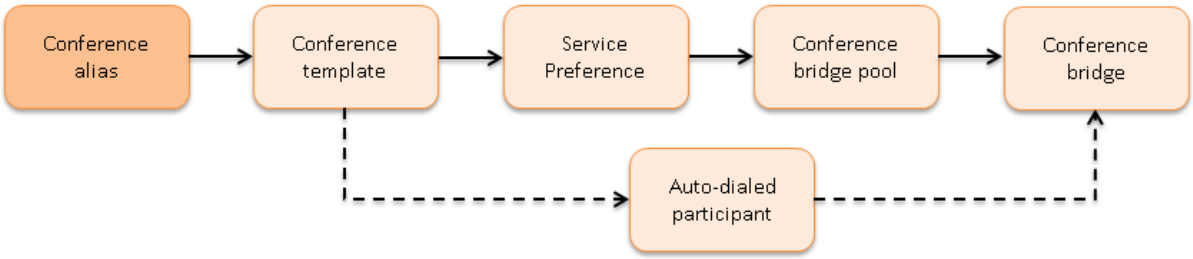
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the conference alias.
Incoming alias	Enter the regex expression to match the incoming string from Unified CM, for example `(6…)@.*` or a more specific pattern. Note that SIP requests received from Unified CM are in the format `name@<IP address | FQDN>:<port>`.
Conference name	Enter a regular expression or create the name of the conference to which this participant will be added.
Priority	Enter the priority for this alias.
Conference template	Select the appropriate template.
Role type	Select *Host*.



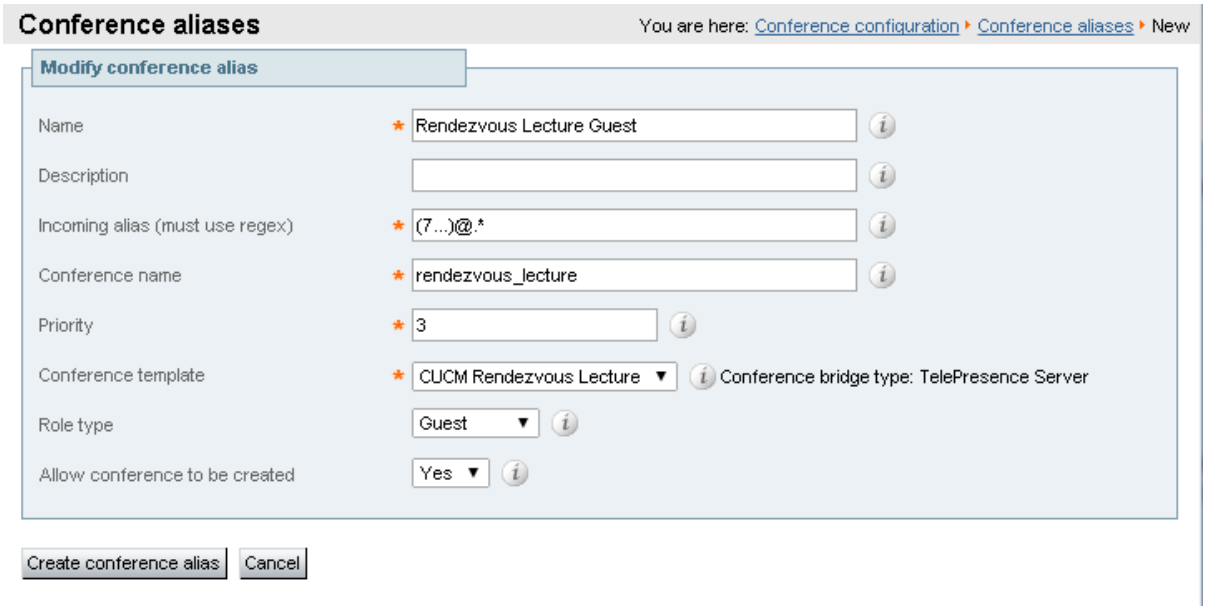
4. Click **Create conference alias**.

Task 27: Creating a guest conference alias for a rendezvous Lecture-type conference



1. Go to **Conference configuration > Conference aliases**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

Name	Enter a name for the conference alias.
Incoming alias	Enter the regex expression to match the incoming string from Unified CM, for example `(7…)@.*` or a more specific pattern. Note that SIP requests received from Unified CM are in the format `name@<IP address | FQDN>:<port>`.
Conference name	Enter a regular expression or create the name of the conference to which this participant will be added.
Priority	Enter the priority for this alias.
Conference template	Select the appropriate template.
Role type	Select *Guest*.



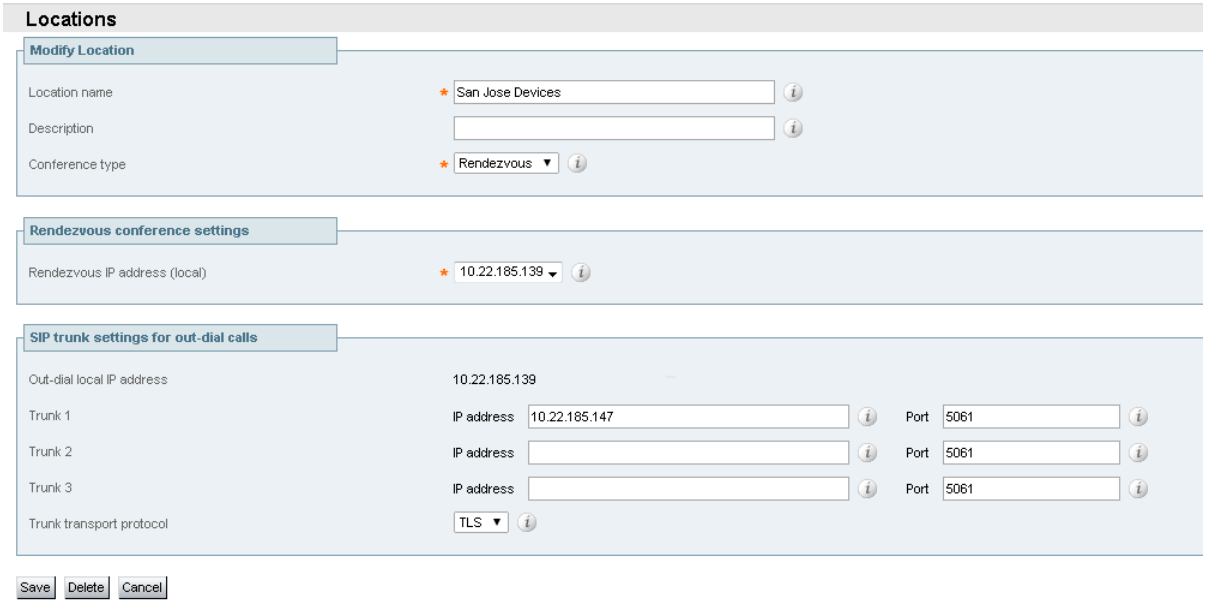
4. Click **Create conference alias**.

Task 28: Creating a rendezvous Location

1. Go to **Conference configuration > Locations**.
2. Click **New**.

3. Enter the following into the relevant fields, leave other fields as their default values:

Location name	Enter a name.
Conference type	Select *Rendezvous* or *Both*, from the drop-down list. In this example *Rendezvous* was selected.
Rendezvous IP address	From the drop-down list, select the TelePresence Conductor IP address to be used for rendezvous calls. This must match the Destination address of the SIP trunk configured on Unified CM.
Trunk 1-3 IP address	This is only required if TelePresence Conductor needs to forward auto-dialed participants or any other out-dialed calls such as those initiated by Cisco TMS to Unified CM. Enter the Unified CM IP address. You can specify up to three trunk IP addresses. Enter the additional trunk IP addresses and ports if you are using a Unified CM cluster. If you specify more than one trunk IP address, the TelePresence Conductor considers all trunk IP addresses for a Location as equivalent. It may use any of the trunk IP addresses defined, as long as the destination is reachable. If the SIP trunk destination that the TelePresence Conductor currently uses becomes unreachable, it will automatically use another reachable destination. The TelePresence Conductor maintains only one of the destinations, it does not load balance the dial-out calls across the configured destinations.
Trunk 1-3 Port	Enter the receiving signaling port of the Unified CM, typically *5061* for TLS and *5060* for TCP.
Trunk transport protocol	Select the transport protocol *TLS* (if Unified CM has version 9.0 or later), otherwise *TCP*.



4. Click **Add location**.

Task 29: Adding Locations to conference bridge pools

When making an outbound call, the TelePresence Conductor needs to send the call to the SIP trunk associated with the location that the conference bridge is in. This configuration will specify the Location for TelePresence Conductor to use when making an outbound call to participants accessible through Unified CM.

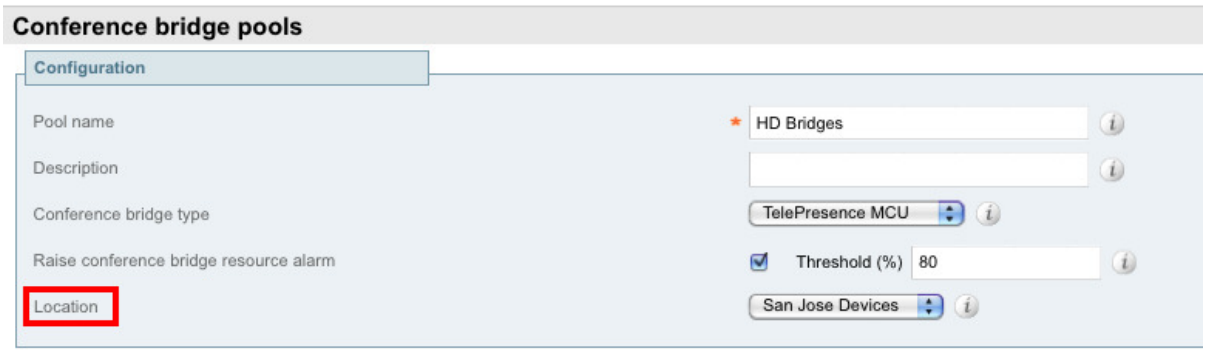
Examples of outbound calls are:

- auto-dialed participants configured on TelePresence Conductor
- Cisco TMS scheduling a conference with participants
- a user of Conference Control Center (CCC) in Cisco TMS adding a participant to an existing conference

The TelePresence Conductor will send the requested dial string to the Unified CM via the SIP trunk associated with that Location. This way Unified CM can enforce CAC bandwidth control as it knows the location of the conference bridge hosting the conference.

To link the conference bridge pool with a Location:

1. Log into the TelePresence Conductor as a user with administrator rights.
2. Go to **Conference configuration > Conference bridge pools**.
3. Click on the relevant conference bridge pool.
4. Select the **Location** to associate with this conference bridge.
   You must first have created at least one Location (see Configuring the TelePresence Conductor [p.26]) in order for it to appear in the drop-down list.
   Leave as *None* if no outbound calls to participants are required from this pool.



5. Repeat steps 2 through 4 for each conference bridge pool.

Configuring Unified CM

The following tasks describe the configuration required on Unified CM. The tasks are split up into:

- general tasks required for both ad hoc and rendezvous conferences
- tasks required for ad hoc conferences only
- tasks for rendezvous conferences only

Configuring general settings on Unified CM

The following tasks are required when configuring either ad hoc or rendezvous conferences or both.

Task 30: Viewing a location in Unified CM

In order to identify which locations should be supported in the TelePresence Conductor, they can be looked up in Unified CM as follows.

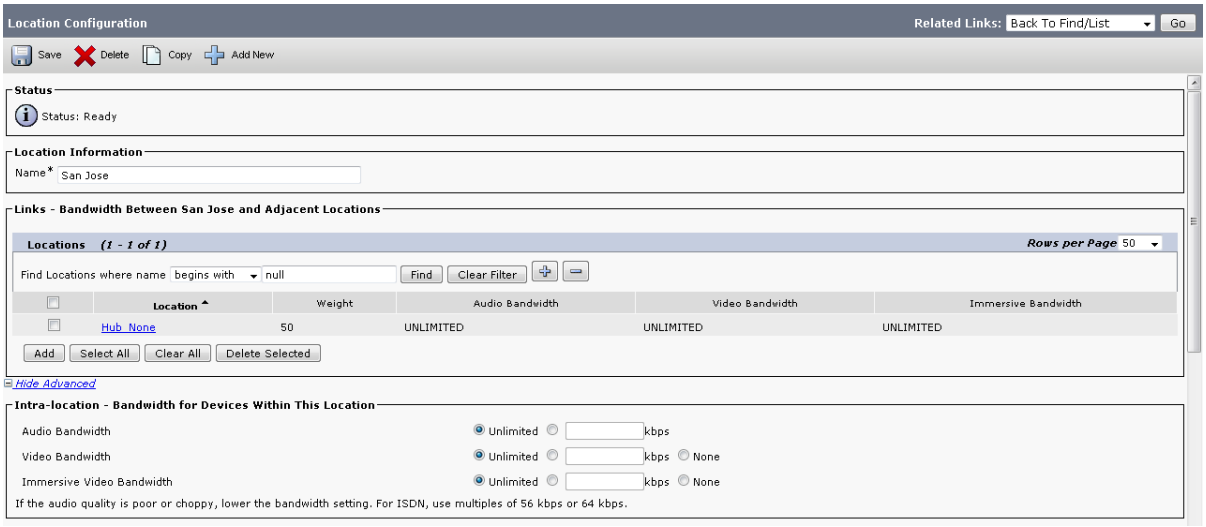
To view a location in Unified CM:

1. Go to the Unified CM web interface and log in as an admin user.
2. Go to **System > Location Info > Location**.
3. Enter a search term, click **Find** and then select the relevant location.
4. The following information will have been configured:

Field	Unified CM version	Input
Name	Pre- 8.6.2 and later	The name of this location.
Video Bandwidth	8.6.2 and prior	The video bandwidth allowed between this location and adjacent locations.
Links - Bandwidth Between <This Location> and Adjacent Locations section	9.0 and later	The video and immersive video bandwidths allowed between this location and adjacent locations are shown.
Show Advanced	9.0 and later	Expand this section to expose options.
Intra-Location -Bandwidth for Devices Within This Location section	9.0 and later	The video and immersive video bandwidths for intra-location (within location) are shown.

Note: In Unified CM version 9.0 or later the bandwidth for TelePresence video (immersive video) and the bandwidth for traditional video can be independently configured. For simplification purposes, the immersive bandwidth refers to all TelePresence based endpoints, such as EX90, C Series, CTS, and

TX9000 and the video bandwidth refers to video enabled telephony endpoints, such as the 8900 and 9900 series phones. For more information on specific models refer to the Unified CM documentation on cisco.com.



Task 31: Ensuring that Unified CM trusts TelePresence Conductor's server certificate and vice versa

For Unified CM and TelePresence Conductor to establish a TLS connection with each other:

- TelePresence Conductor and Unified CM must both have valid server certificates loaded (you must replace the TelePresence Conductor's default server certificate with a valid server certificate)
- TelePresence Conductor must trust Unified CM's server certificate (the root CA of the Unified CM server certificate must be loaded onto TelePresence Conductor)
- Unified CM must trust TelePresence Conductor's server certificate (the root CA of the TelePresence Conductor server certificate must be loaded onto Unified CM)

See Appendix 4: Ensuring that Unified CM trusts TelePresence Conductor's server certificate and vice versa [p.96] in this document for more information on how to ensure that Unified CM trusts the TelePresence Conductor server certificate.

See *Cisco TelePresence Conductor Certificate Deployment Guide* for full details about loading certificates and how to generate CSRs on TelePresence Conductor to acquire certificates from a Certificate Authority (CA).

Note: In a clustered environment, you must install CA and server certificates on each peer/node individually.

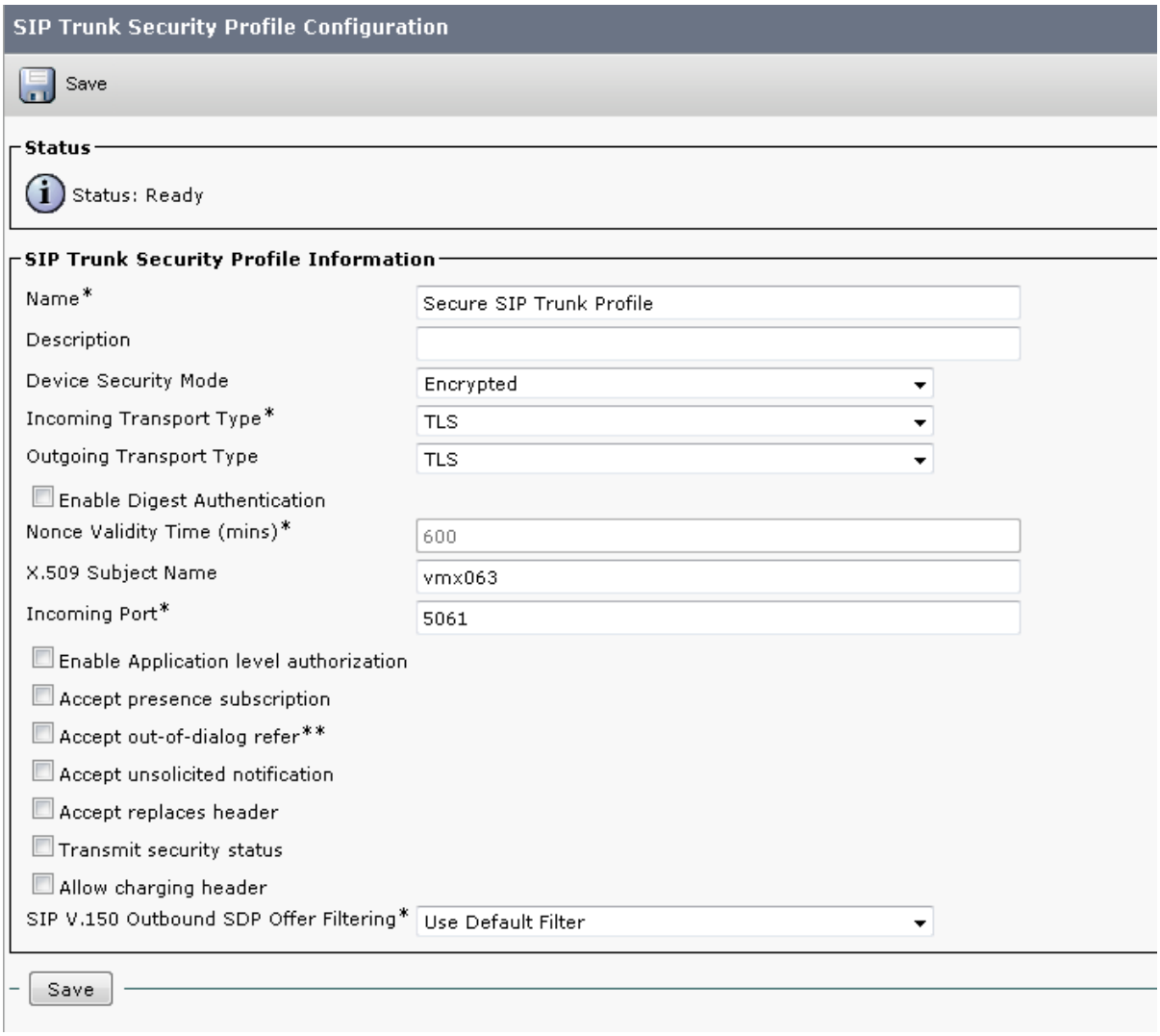
We strongly recommend that you do not use self-signed certificates in a production environment.

Task 32: Ensuring that a secure SIP trunk security profile is configured

On the Unified CM go to **System > Security > SIP Trunk Security Profile** and check if a new profile is needed. If so:

1. Click **Add New**.
2. Enter the following in the relevant fields:

Name	A name indicating that this profile is an encrypted profile for the specific X.509 name(s).
Description	Enter a textual description as required.
Device Security Mode	Select *Encrypted*.
Incoming Transport Type	Select *TLS*.
Outgoing Transport Type	Select *TLS*.
Enable Digest Authentication	Leave unselected.
X.509 Subject Name	The subject name or an alternate subject name provided by the TelePresence Conductor in its certificate. (Multiple X.509 names can be added if required; separate each name by a space, comma, semicolon or colon.)
Incoming Port	Enter '5061'.
Other parameters	Leave all other parameters unselected.



3. Click **Save**.

Task 33: Creating a new SIP profile

When creating the SIP profile, the time for **Timer Invite Expires (seconds)** should be configured to match the TelePresence Conductor's operation. TelePresence Conductor will wait up to 30 seconds from acknowledging the ad hoc conference request from Unified CM to receiving a call for that conference. To create a new SIP profile:

1. On Unified CM, go to **Device > Device Settings > SIP Profile**.
2. Click on the **Copy** button to the right of the Standard SIP Profile for TelePresence Conferencing.
   This will create a new SIP profile with the same settings as the Standard SIP Profile for TelePresence Conferencing.
3. In the **Name** field, enter `SIP Profile for Conductor`.

4. Under the **Parameters used in Phone** section, change the **Timer Invite Expires (seconds)** to '30'.
5. Click **Save**.

Configuring Unified CM for ad hoc conferences

The following tasks are required when configuring ad hoc conferences.

Note: The phone/endpoint used to initiate an ad hoc conference must have a conference button. Phones/endpoints that do not have a conference button may still be participants in an ad hoc conference, but they must be added to the conference by a phone/endpoint that has a conference button.

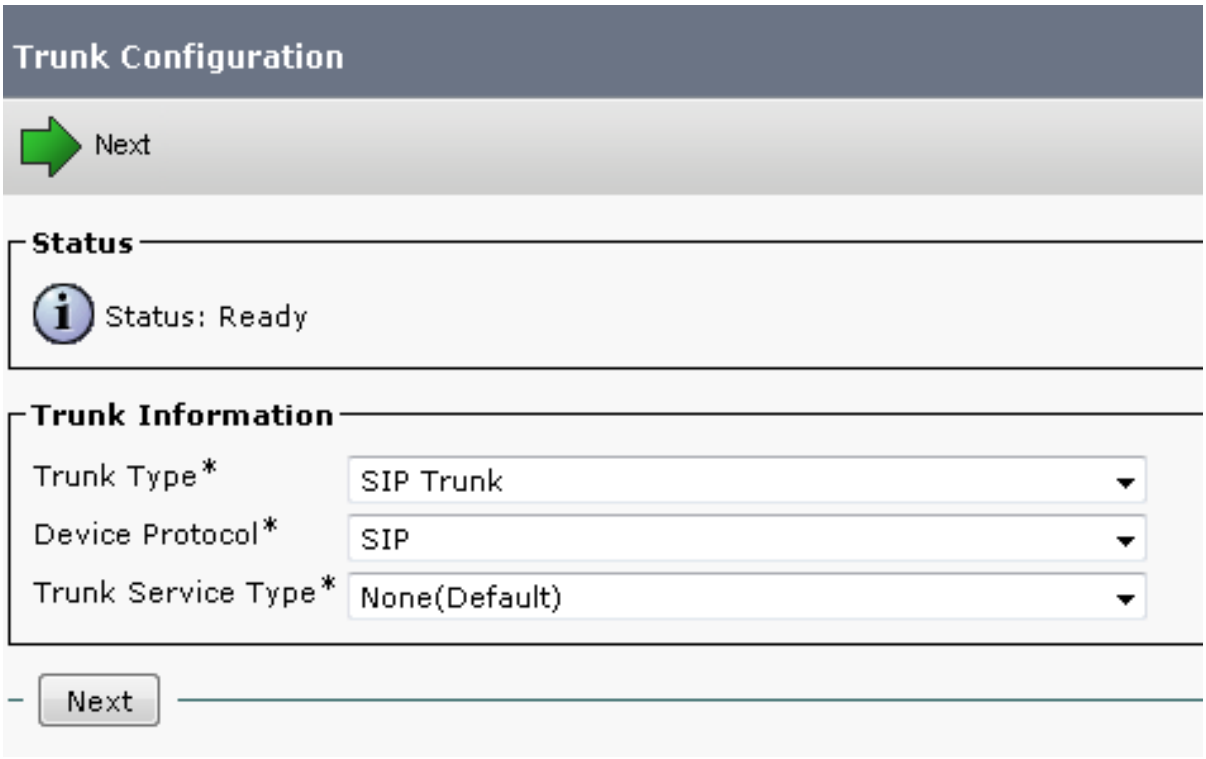
Task 34: Adding a SIP trunk connecting to TelePresence Conductor

From Unified CM version 10.x onwards a SIP trunk between Unified CM and TelePresence Conductor must be explicitly configured for ad hoc conferences. The task is not required when running an earlier version of Unified CM.

To configure a SIP trunk connecting to the TelePresence Conductor for ad hoc conferences:

1. Go to **Device > Trunk**.
2. Click **Add New** to create a new SIP trunk.
3. Enter the following into the relevant fields:

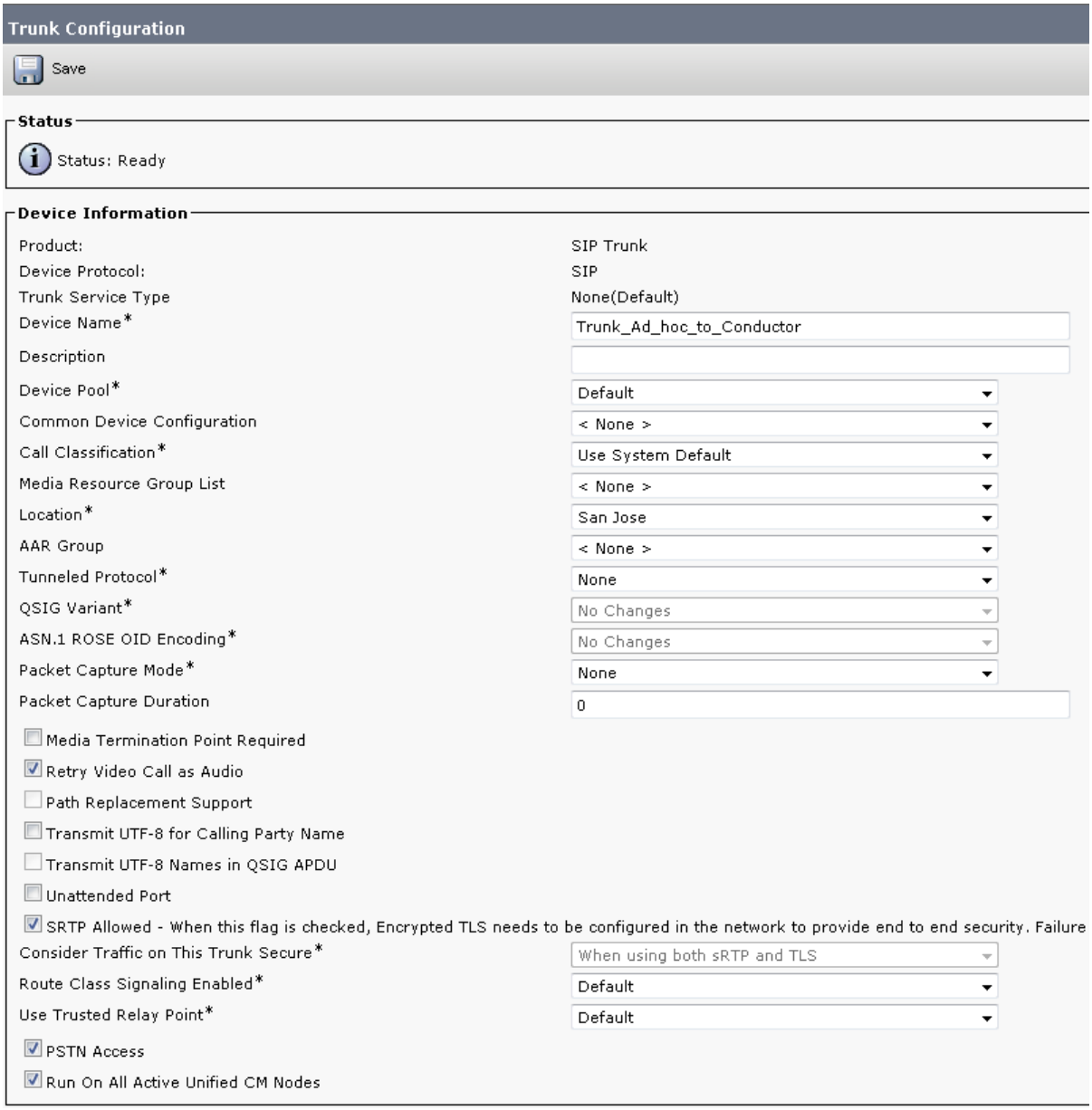
Trunk Type	Select *SIP Trunk*.
Device Protocol	Leave as default: *SIP*.
Trunk Service Type	Leave as: *None(Default)*.

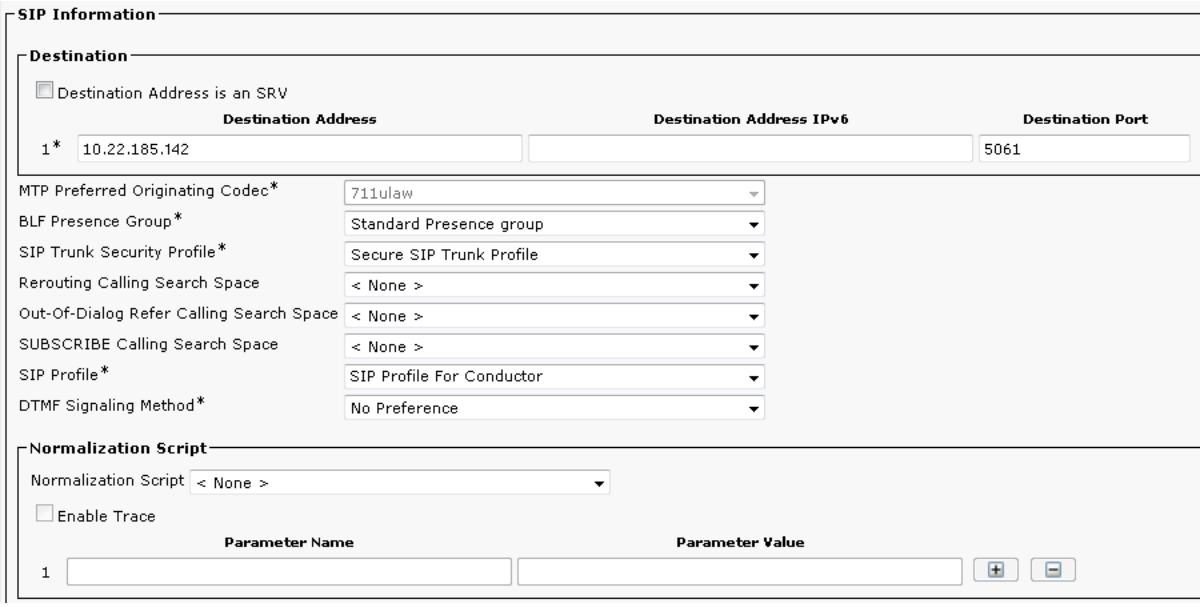


4. Click **Next**.
5. Enter the following into the relevant fields, leave other fields as their default values:

Device Information section	
Device Name	Enter a trunk name.
Device Pool	Select the appropriate Device Pool.
Location	Select the Location found in Task 30: Viewing a location in Unified CM [p.50].
SRTP Allowed	Check this setting.
Run On All Active Unified CM Nodes	Check this setting.
SIP Information section	
Destination Address	Enter the TelePresence Conductor's Location-specific ad hoc IP address. This IP address is the ad hoc IP address configured in the **Additional addresses for LAN1** section on the TelePresence Conductor's **IP** page (**System > Network interfaces > IP**). (See Task 18: Adding IP addresses for ad hoc and rendezvous locations on TelePresence Conductor [p.35])
Destination Port	Enter '5061'.

SIP Trunk Security Profile	Select the *Secure SIP Trunk Profile* from the drop-down list.
SIP Profile	Select the SIP Profile created in Task 33: Creating a new SIP profile [p.53].





6. Click **Save**.
7. Click **Reset**.

Task 35: Adding the TelePresence Conductor as a Conference bridge to Unified CM

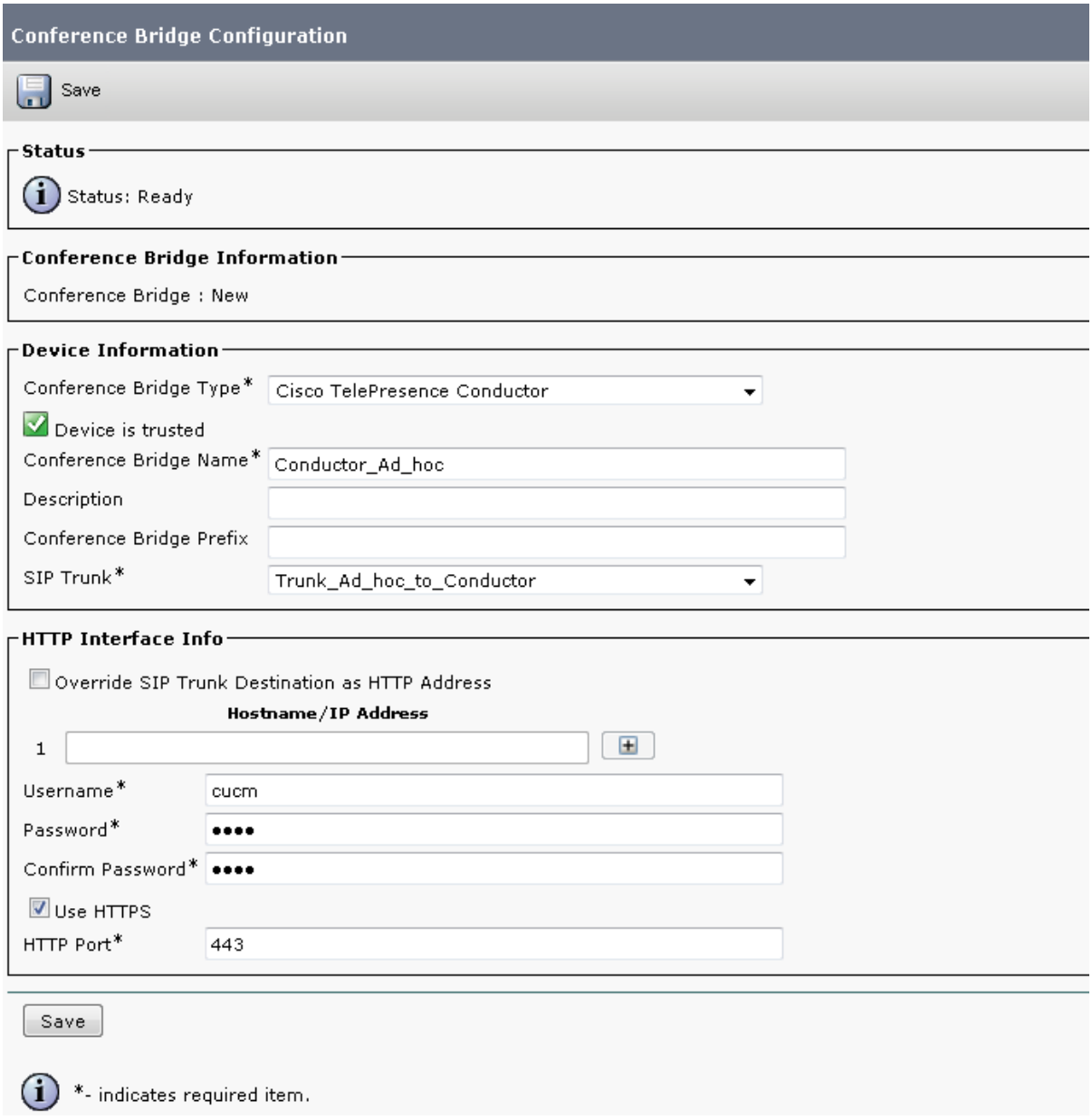
Note: The instructions in this task are for Unified CM version 10.x. For Unified CM version 8.6.2, go to Appendix 1: Unified CM version 8.6.2 configuration [p.90] and for Unified CM version 9.x, go to Appendix 2: Unified CM version 9.x configuration [p.92].

For Unified CM version 10.x:

1. Go to **Media Resources > Conference Bridge**.
2. Click **Add New** to create a new Conference Bridge.
3. Enter the following into the relevant fields, leave other fields as their default values:

Device Information section	
Conference Bridge Type	Select *Cisco TelePresence Conductor*.
Conference Bridge Name	Enter a descriptive name for the TelePresence Conductor.
SIP Trunk	Select from the drop-down list the SIP Trunk for ad hoc conferences created in Task 34: Adding a SIP trunk connecting to TelePresence Conductor [p.54].

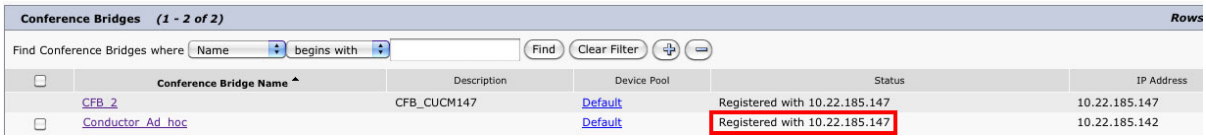
HTTP Interface Info section	
Username	Enter the username of the TelePresence Conductor administration user set up earlier. This appears on the TelePresence Conductor's **Administrator accounts** page (**Users > Administrator accounts**).
Password	Enter the password of the TelePresence Conductor administration user.
Use HTTPS	We recommend that you tick this box.
HTTP Port	Enter '443'.



Click **Save**.

Click **Reset**.

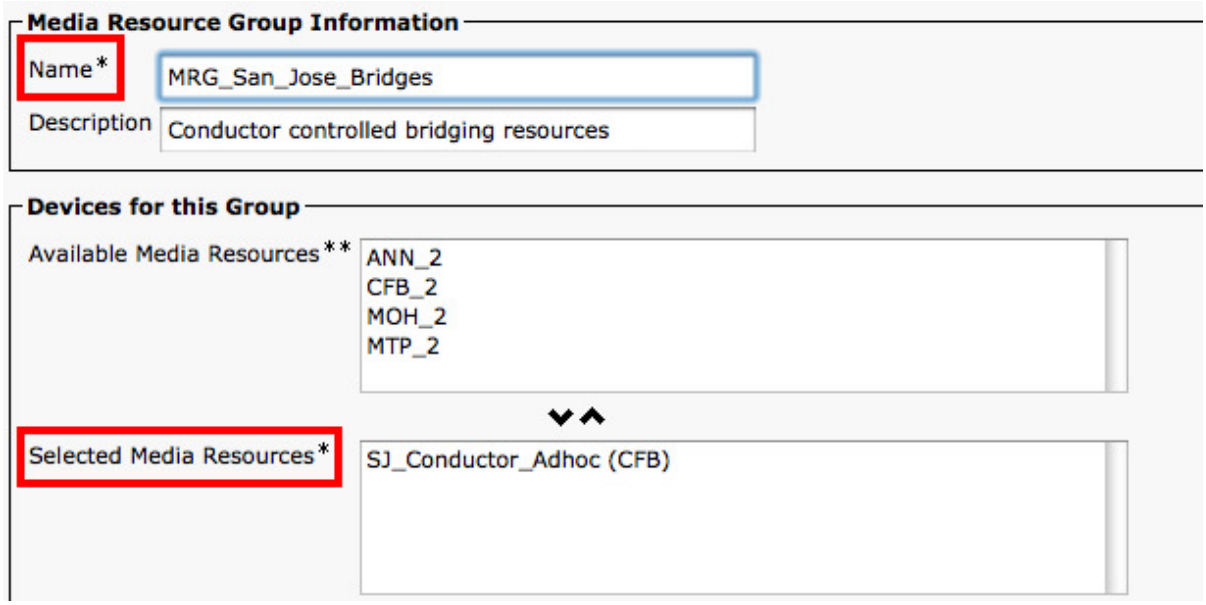
4. Find the **Related Links: Back to Find/List** and click **Go**.
5. Verify that the TelePresence Conductor is registered with Unified CM.



Task 36: Adding the TelePresence Conductor to an MRG and MRGL

To configure the Unified CM with the TelePresence Conductor in a Media Resource Group (MRG):

1. Go to **Media Resources> Media Resource Group**.
2. Click **Add New** to create a new media resource group.
3. Enter a name for the MRG.
4. Move the TelePresence Conductor media bridge (the conference bridge configured in Task 35: Adding the TelePresence Conductor as a Conference bridge to Unified CM [p.57]) down to the **Selected Media Resources** box.

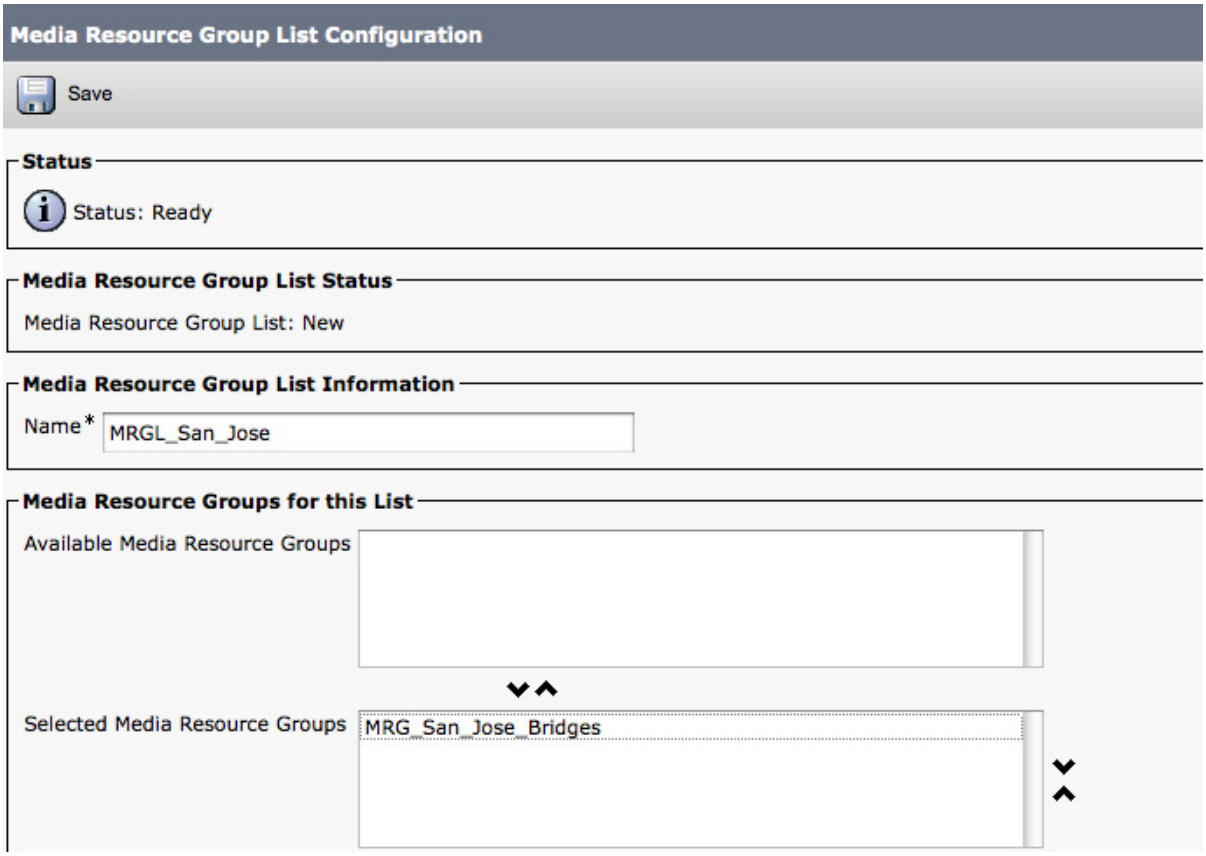


5. Click **Save**.

To configure a Media Resource Group List (MRGL) in Unified CM:

6. Go to **Media Resources > Media Resource Group List**.
7. Click **Add New** to create a new media bridge group or find an existing MRGL and click on it to edit it.
8. Enter a name for the MRGL.

9. Move the TelePresence Conductor media bridge group configured in steps 2 – 5 above, down to the **Selected Media Resource Groups** box.



10. Click **Save**.

Task 37: Adding an MRGL to a Device Pool or Device

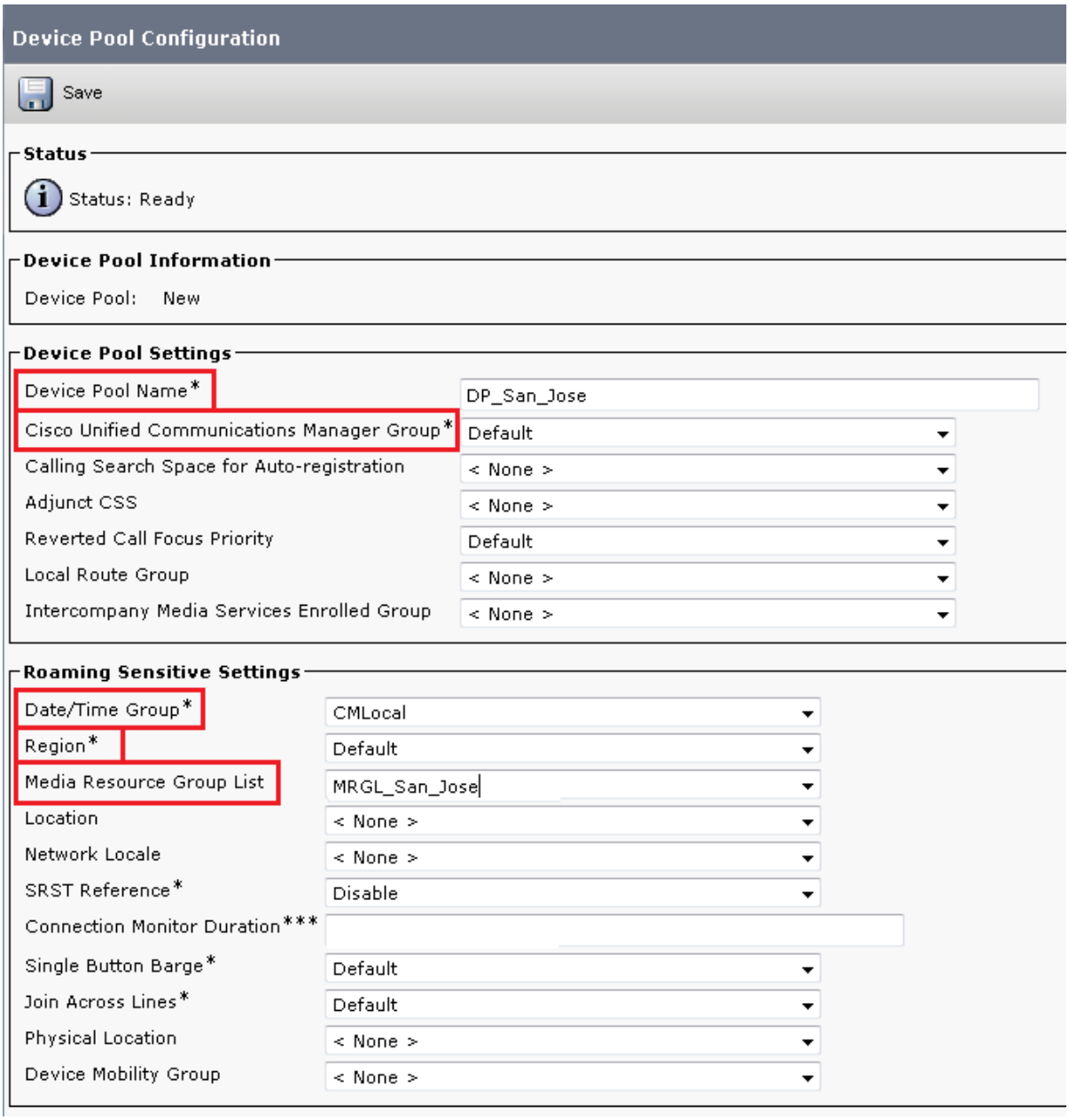
Depending on the implementation, either a Device Pool can be configured and applied to all endpoints, or an individual device (i.e. an endpoint) can be assigned a specific MRGL. If a MRGL is applied to both a Device Pool and an endpoint, the endpoint setting will be used. For further information on Device Pools or Devices reference the Unified CM documentation on cisco.com.

To configure Media Bridge Group List (MRGL) to a Device Pool:

1. Go to **System > Device Pool**.
2. Click **Add New** to create a new Device pool or find a Device pool and click on it to edit an existing pool.
3. Enter the following into the relevant fields, leave other fields as their default (or previously configured) values:

Device Pool Settings section

Device Pool Name	Enter a Device pool name.
Cisco Unified Communications Manager Group	Select the appropriate group from the drop-down list.
Roaming Sensitive Settings section	
Date/Time Group	Select the appropriate group from the drop-down list.
Region	Select the appropriate region from the drop-down list.
Media Resource Group List	Select the MRGL created in Task 36: Adding the TelePresence Conductor to an MRG and MRGL [p.59] (steps 6 -10) from the drop-down list.

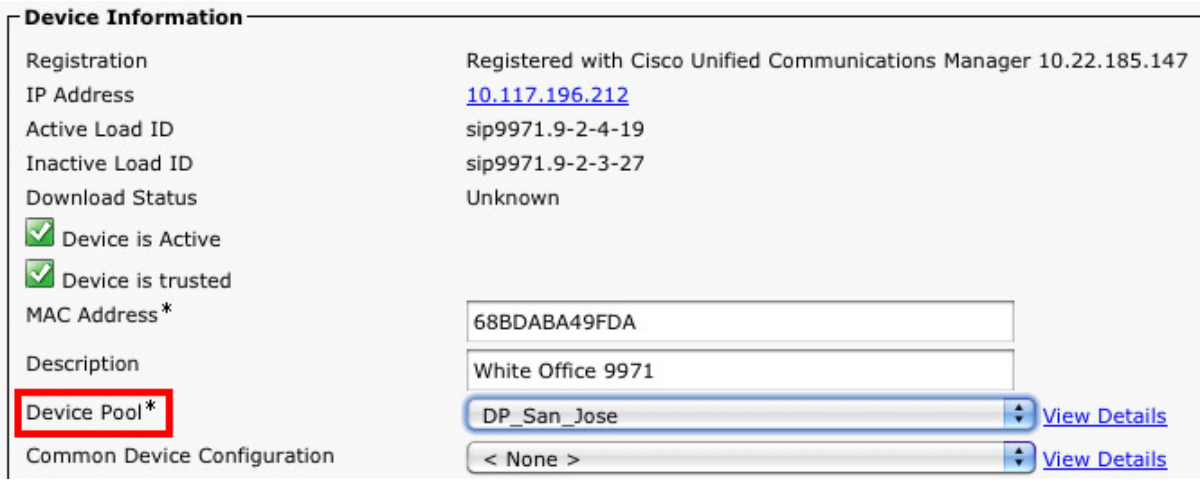


4. Click **Save** and **Reset** for the changes to take effect.

Note: If there are devices associated with the pool, they will reboot when **Reset** is clicked.

If a new Device pool has been created:

5. Go to **Device > Phones**.
6. Click **Find** and select the device to change the Device Pool settings on.
7. Select the Device Pool used above (in steps 1-4) from the drop-down list.

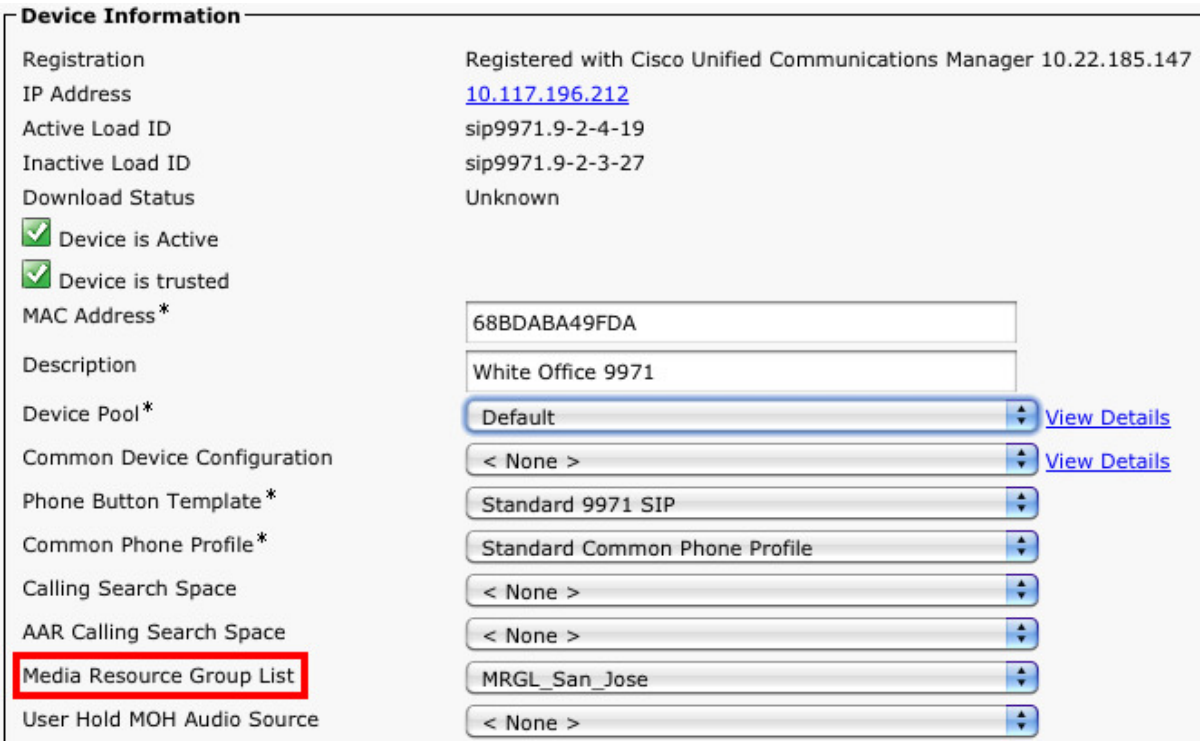


8. Click Save.
9. Click **Apply Config**.
10. Click **Reset** for the changes to take effect.
    Note: This will reboot the phones when applied.

To apply an MRGL directly to a device or endpoint as opposed to using a Device Pool do the following:

Note: The MRGL setting closest to the device will be the active setting. For example, if the endpoint has a Device Pool assigned to it, which had an MRGL defined within the Device Pool, and the endpoint has another MRGL selected at the device level, the device level setting will be used.

1. Go to **Device > Phones**.
2. Click **Find** and select the device to change the MRGL settings on.
3. Select the MRGL used in Task 36: Adding the TelePresence Conductor to an MRG and MRGL [p.59] (steps 6 – 10) from the drop-down list.



4. Click **Save**.
5. Click **Apply Config**.
6. Click **Reset** for the changes to take effect.

Task 38: Adding the Unified CM normalization script

Follow the instructions in Appendix 3: Adding the Unified CM normalization script [p.94] to add the Unified CM normalization script to Unified CM.

Configuring Unified CM for rendezvous conferences

The following tasks are required when configuring rendezvous conferences.

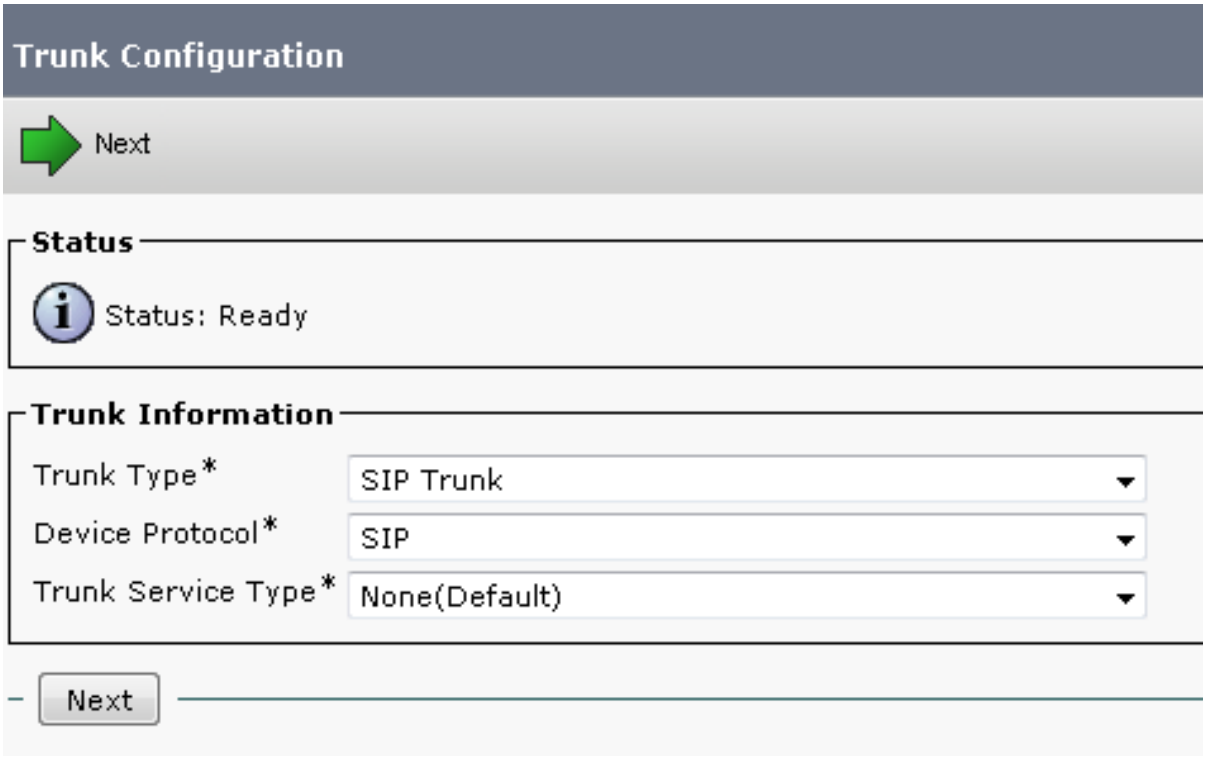
Task 39: Adding a SIP trunk connecting to TelePresence Conductor

To configure a SIP trunk connecting to the TelePresence Conductor for rendezvous conferences:

1. Go to **Device > Trunk**.
2. Click **Add New** to create a new SIP trunk.

3. Enter the following into the relevant fields:

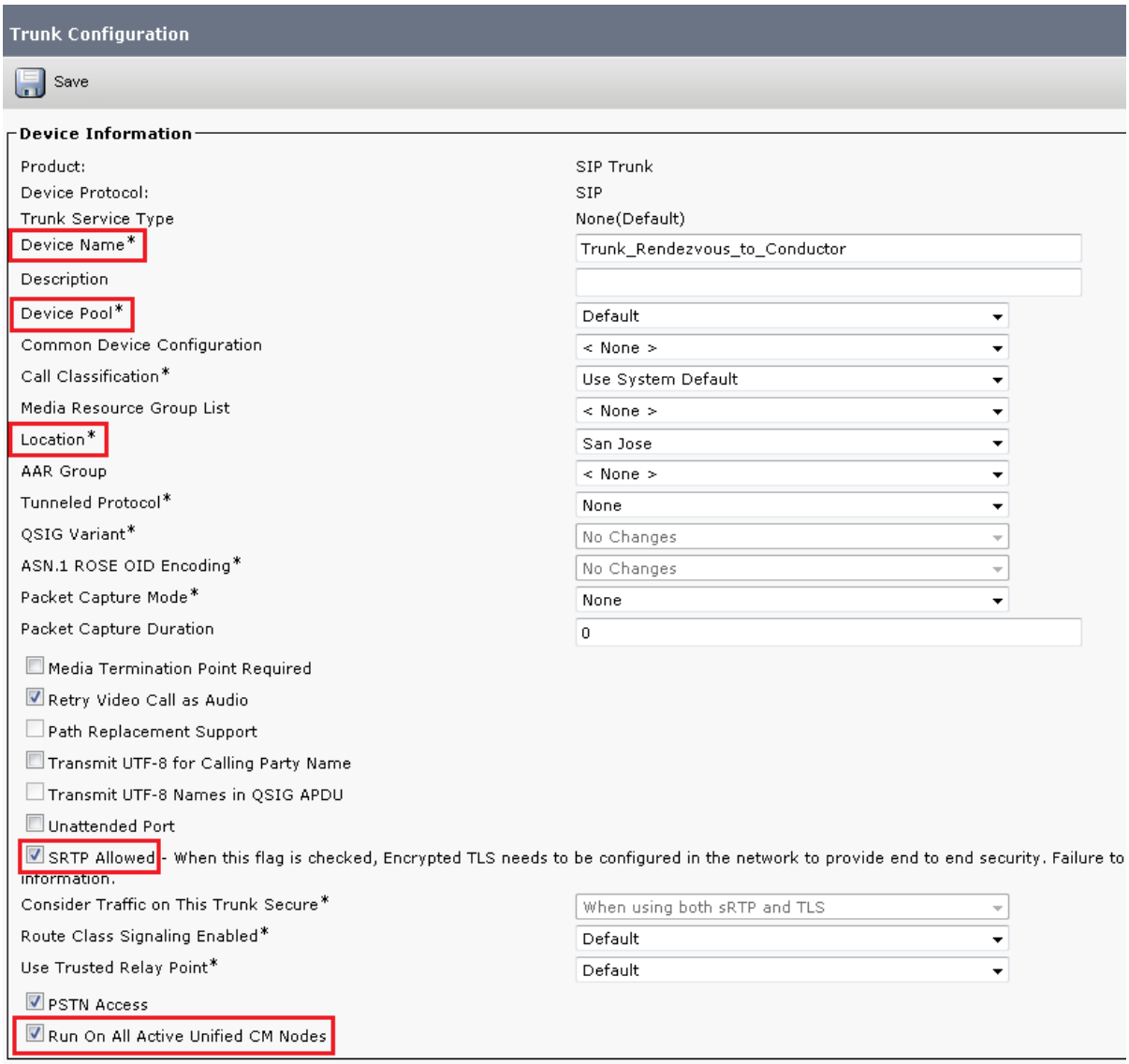
Trunk Type	Select *SIP Trunk*.
Device Protocol	Leave as default: *SIP*.
Trunk Service Type	Leave as: *None(Default)*.

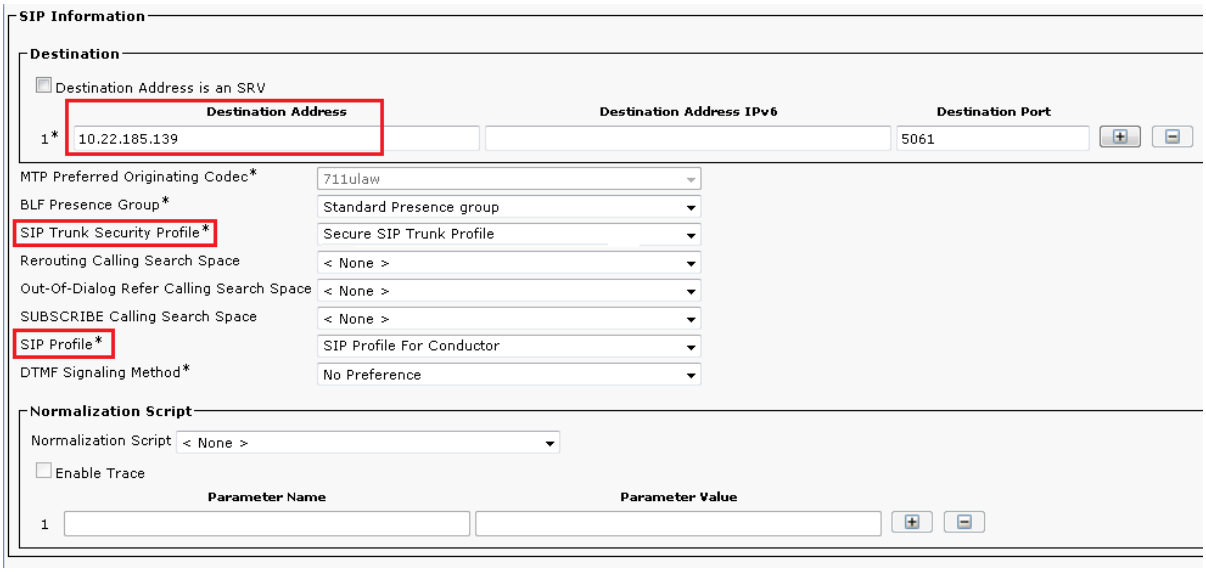


4. Click **Next**.
5. Enter the following into the relevant fields, leave other fields as their default values:

Device Information section	
Device Name	Enter a trunk name.
Device Pool	Select the appropriate Device Pool.
Location	Select the Location found in Task 30: Viewing a location in Unified CM [p.50].
SRTP Allowed	Check this setting.
Run On All Active Unified CM Nodes	Check this setting.

SIP Information section	
Destination Address	Enter the TelePresence Conductor's Location-specific rendezvous IP address. This IP address is the rendezvous IP address configured in the **Additional addresses for LAN1** section on the TelePresence Conductor's **IP** page (**System > Network interfaces > IP**). (See Task 18: Adding IP addresses for ad hoc and rendezvous locations on TelePresence Conductor [p.35])
Destination Port	Enter '5061'.
SIP Trunk Security Profile	Select the *Secure SIP Trunk Profile* from the drop-down list.
SIP Profile	Select the SIP Profile created in Task 33: Creating a new SIP profile [p.53].





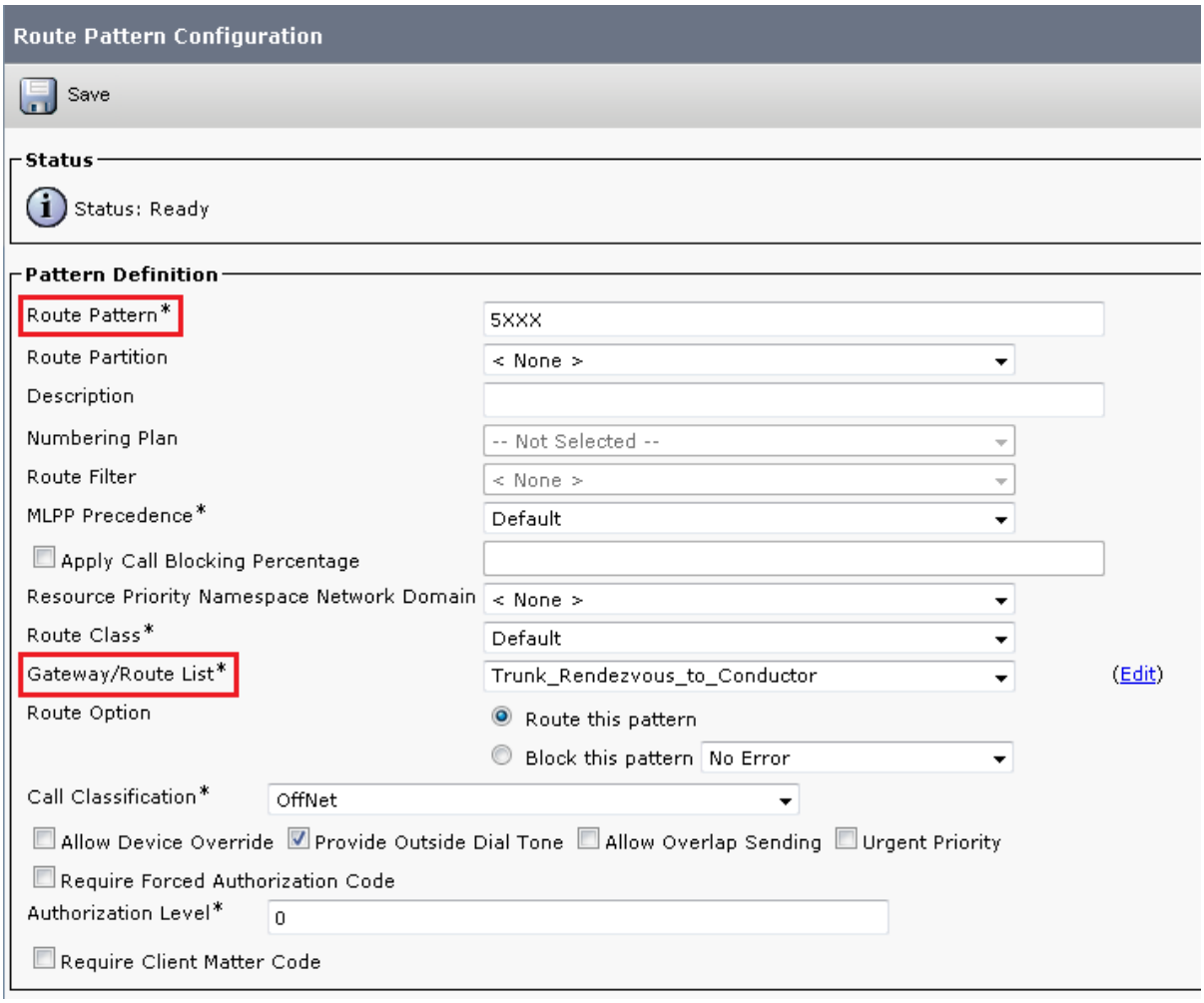
6. Click **Save**.
7. Click **Reset**.

Task 40: Adding a route pattern to match the SIP trunk connecting to TelePresence Conductor

To configure a route pattern to match the SIP trunk connecting to the TelePresence Conductor for rendezvous calls:

1. Go to **Call Routing > Route/Hunt > Route Pattern**.
2. Click **Add New** to create a new route pattern.
3. Enter the following into the relevant fields, leave other fields as their default values:

Route Pattern	Enter a route pattern to match against the destination string.
Gateway/Route List	Select the trunk created in Task 39: Adding a SIP trunk connecting to TelePresence Conductor [p.63].



4. Click **Save**.

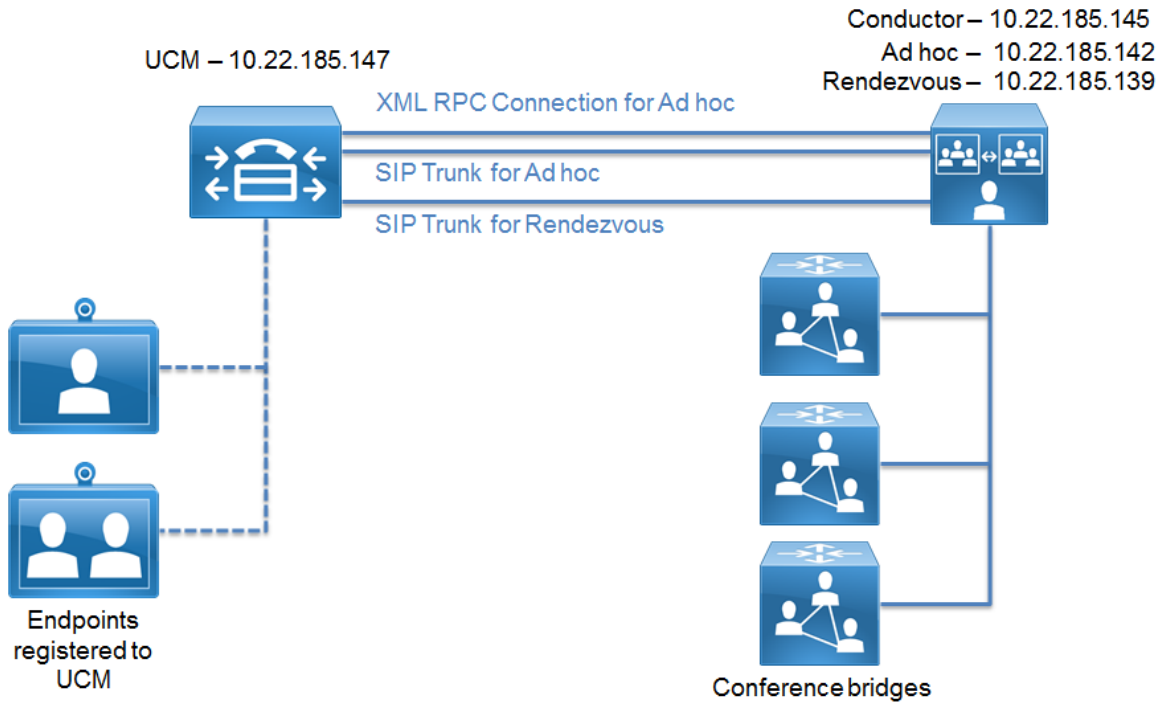
Task 41: Adding the Unified CM normalization script

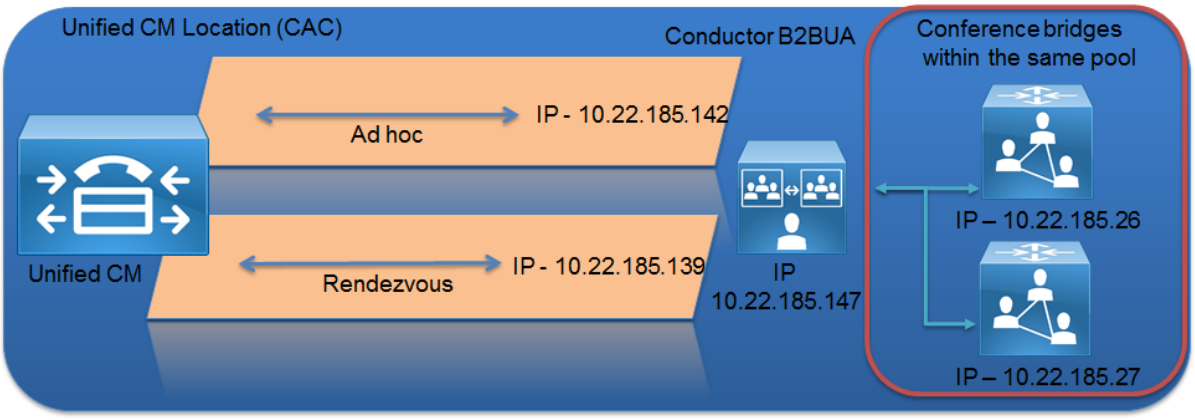
(This task is not required if Task 38: Adding the Unified CM normalization script [p.63] has already been configured for rendezvous conferences.)

Follow the instructions in Appendix 3: Adding the Unified CM normalization script [p.94] to add the Unified CM normalization script to Unified CM.

Testing system configuration

Once you have completed the configuration described in the previous sections, you should test that the system is working correctly. The diagram below is a reference for the testing steps:



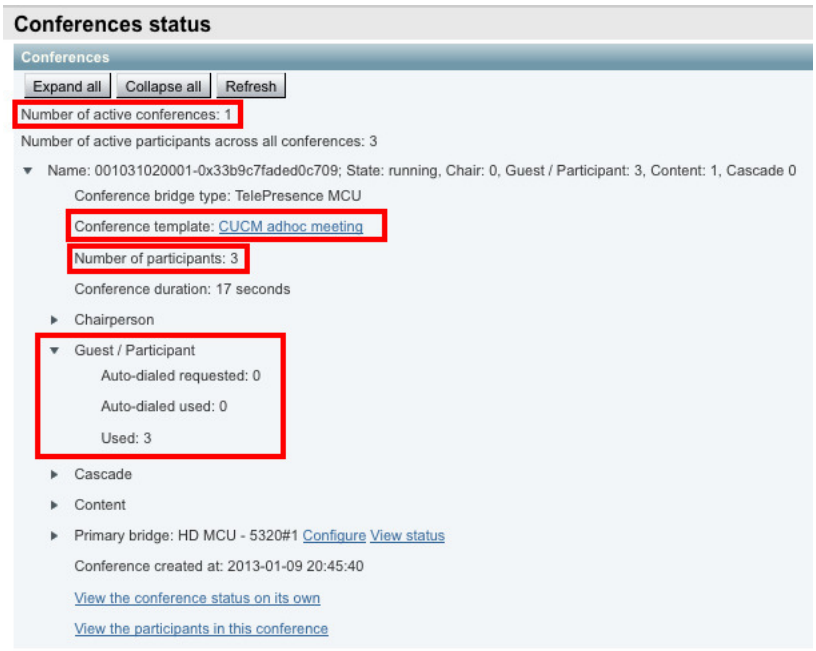


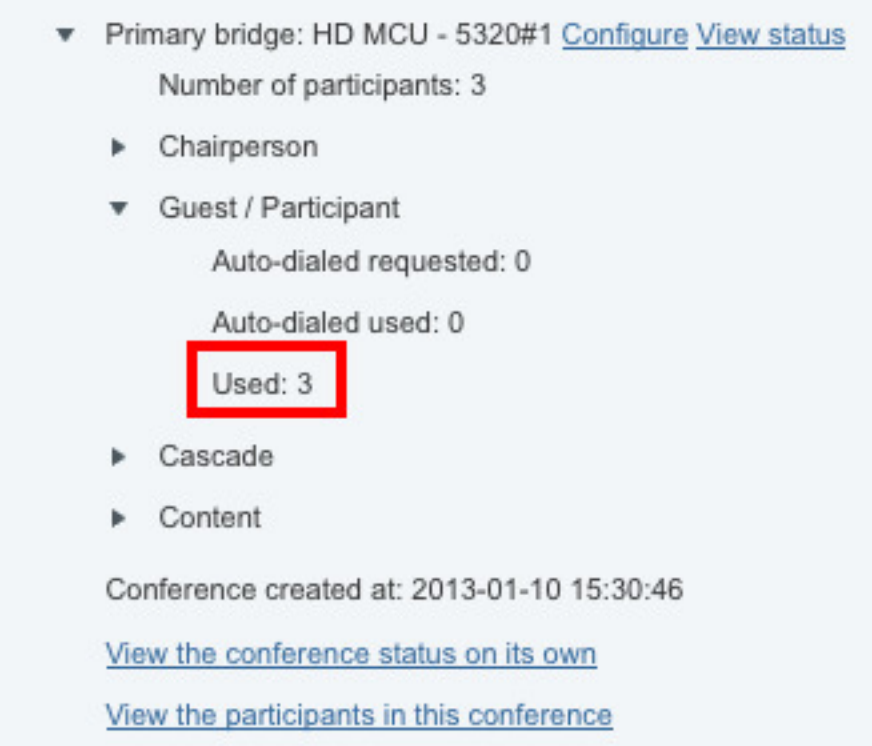
Note: The following examples assume that a conference template based on a TelePresence MCU conference bridge has been used.

Creating an ad hoc meeting

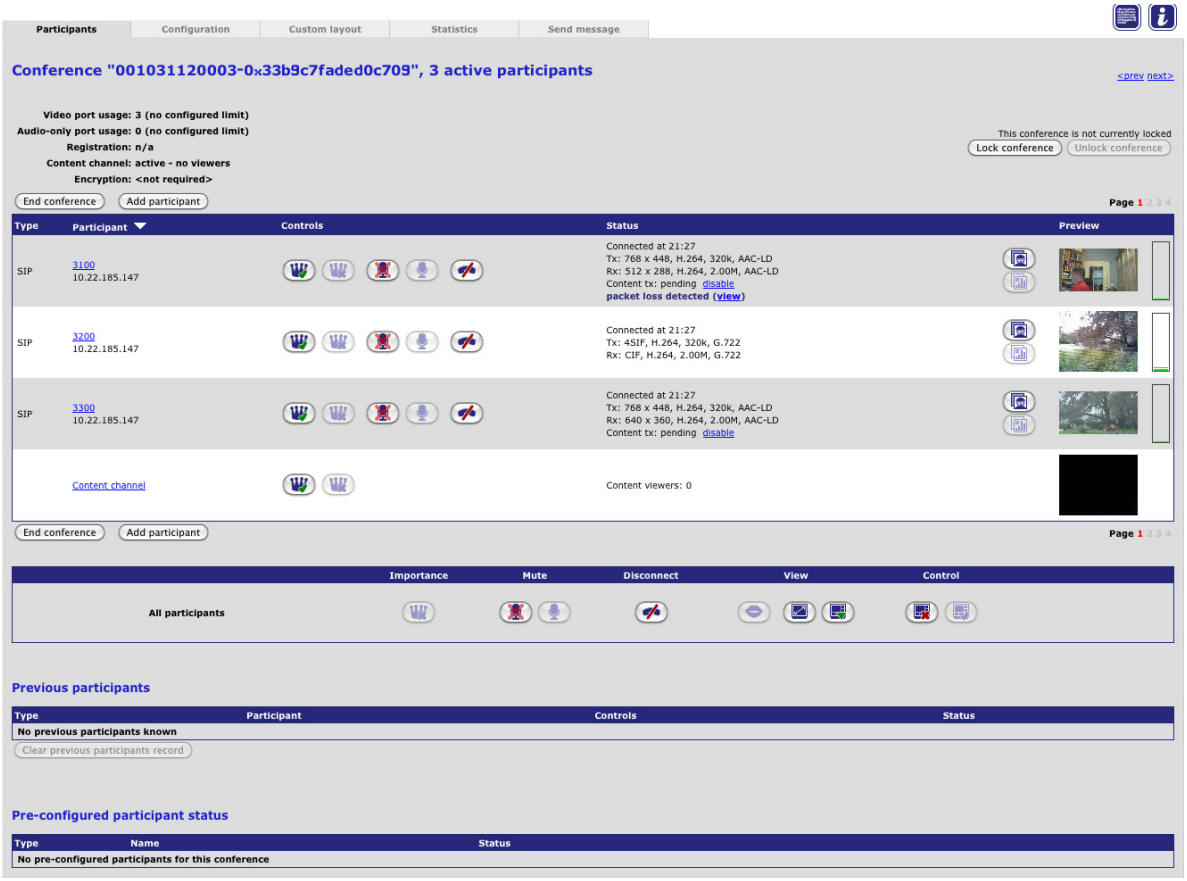
To test that three Unified CM-registered endpoints can join an ad hoc conference that is based on a TelePresence Conductor template with a type of *Meeting*, perform the following steps:

1. From endpoint A dial 3100. Verify a video and audio session is established between endpoint A and endpoint B.
2. From endpoint A, press the conference button and dial 3300. Verify a video and audio session is established between endpoint A and endpoint C. The call between endpoint A and endpoint B has been put on hold.
   Note: At this point the TelePresence Conductor is not involved.
3. From endpoint A press the **Conference** tab on the screen to join the participants and move the call to a conference bridge.
   The call is now established on the TelePresence MCU via the TelePresence Conductor's B2BUA.
4. To verify the established call on the TelePresence Conductor, go to **Status > Conferences**.


Conferences status
Conferences
Expand all
Collapse all
Refresh
Number of active conferences: 1
Number of active participants across all conferences: 3
Name: 001031020001-0x33b9c7faded0c709; State: running, Chair: 0, Guest / Participant: 3, Content: 1, Cascade 0
Conference bridge type: TelePresence MCU
Conference template: CUCM adhoc meeting
Number of participants: 3
Conference duration: 17 seconds
Chairperson
Guest / Participant
Auto-dialed requested: 0
Auto-dialed used: 0
Used: 3
Cascade
Content
Primary bridge: HD MCU - 5320#1 Configure View status
Conference created at: 2013-01-09 20:45:40
View the conference status on its own
View the participants in this conference


Primary bridge: HD MCU - 5320#1 Configure View status
Number of participants: 3
Chairperson
Guest / Participant
Auto-dialed requested: 0
Auto-dialed used: 0
Used: 3
Cascade
Content
Conference created at: 2013-01-10 15:30:46
View the conference status on its own
View the participants in this conference

5. To verify the established call on the TelePresence MCU, go to the **Conference Status** page (**Conferences** on the main tab).

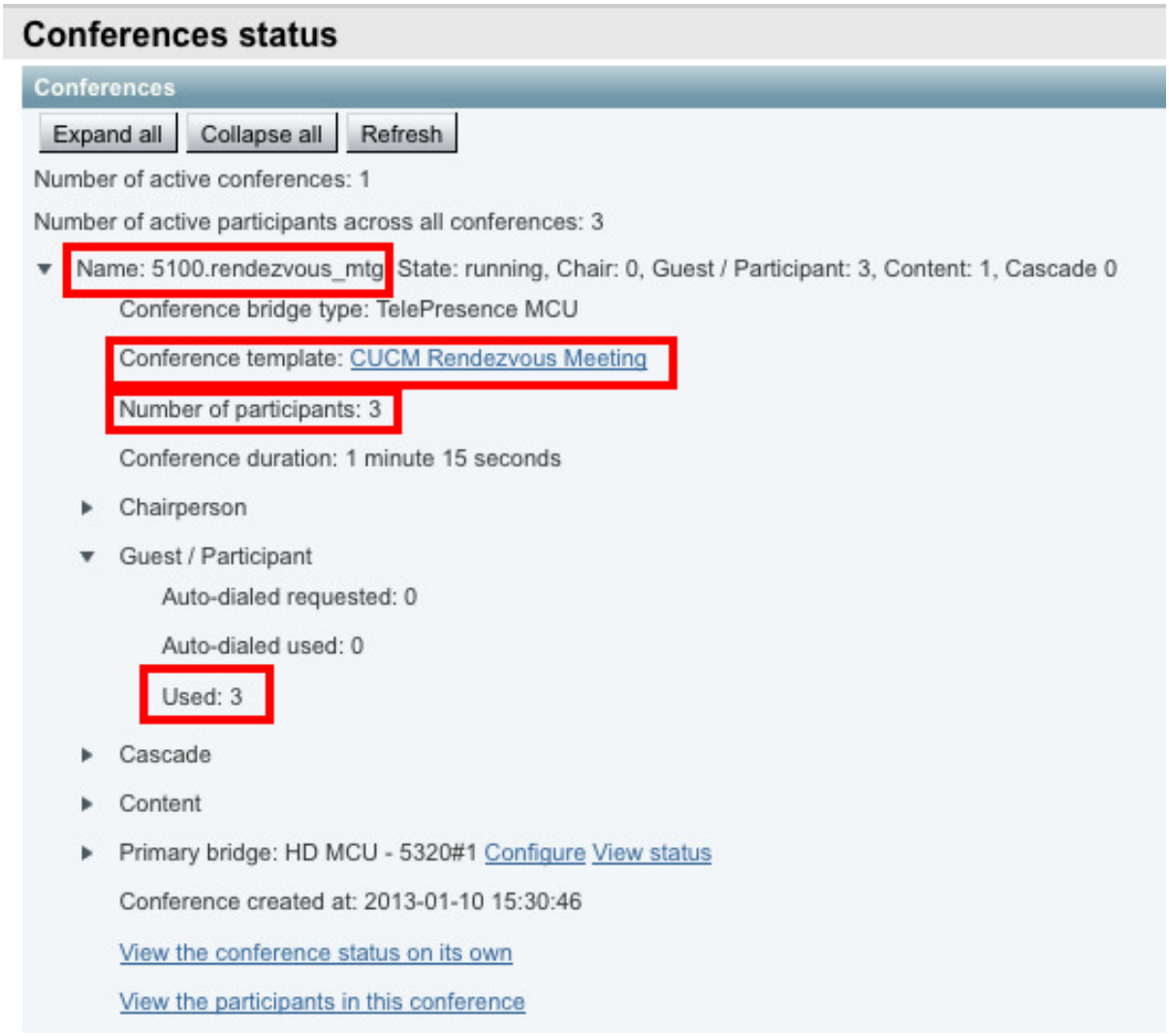


Creating a rendezvous meeting

To test that two or more Unified CM-registered endpoints can join a rendezvous HD conference that is based on a TelePresence Conductor template with a type of *Meeting*, perform the following steps:

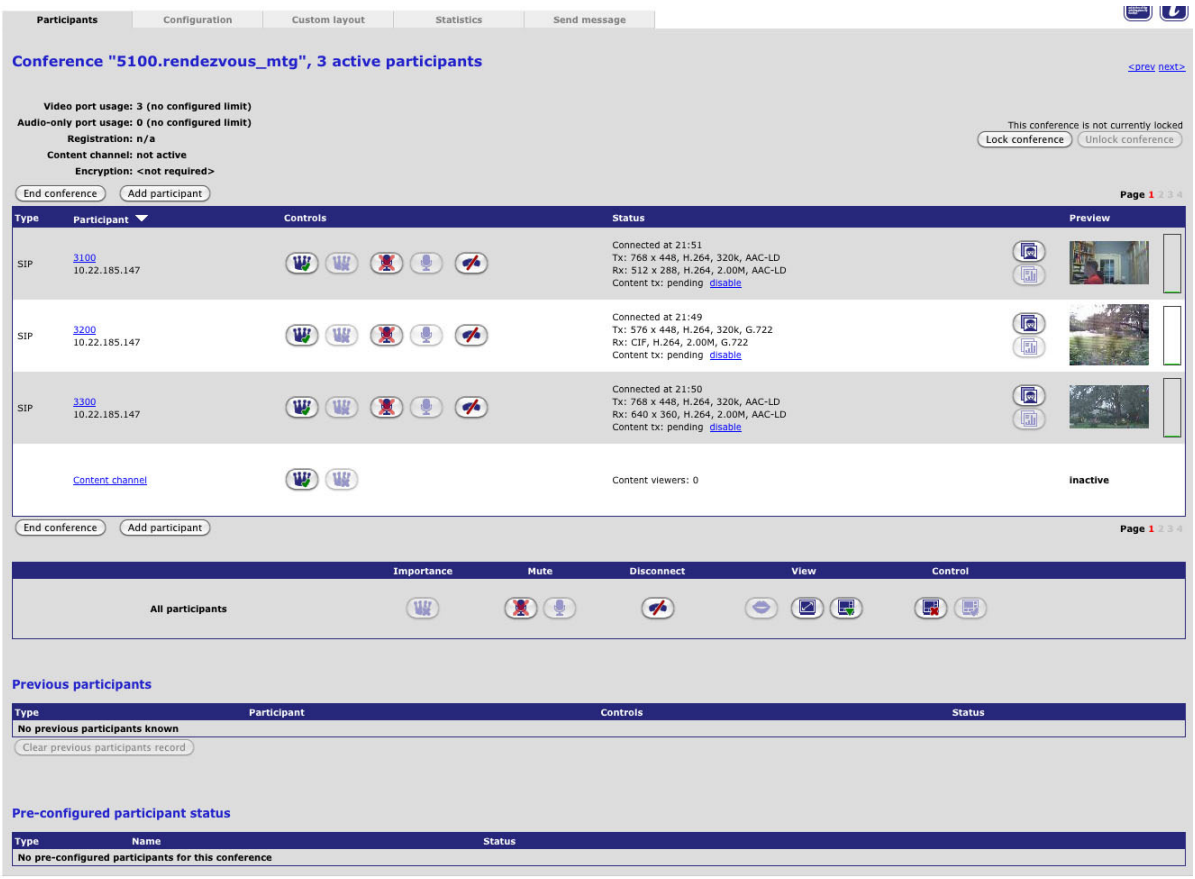
1. From endpoint A dial 5100. This will match the route pattern 5XXX that is associated with the SIP trunk to the TelePresence Conductor. Verify a video and audio session is established with the TelePresence MCU. An audio response of “You are the first participant to join” will be heard.
2. From the endpoint B dial 5100. Verify a video and audio session is established between endpoint B and the TelePresence MCU.
3. From the endpoint C dial 5100. Verify a video and audio session is established between endpoint C and the TelePresence MCU.
4. Each participant should be seeing video of the other participants’ camera and hearing audio from the other endpoints.

5. To verify on the TelePresence Conductor that the call is passed through the B2BUA, go to **Status > Conferences**.



Primary bridge: HD MCU - 5320#1 Configure View status
Number of participants: 3
Chairperson
Guest / Participant
Auto-dialed requested: 0
Auto-dialed used: 0
Used: 3
Cascade
Content
Conference created at: 2013-01-10 15:30:46
View the conference status on its own
View the participants in this conference

6. To verify the established call on the TelePresence MCU, go to the **Conference Status** page (**Conferences** on the main tab).



Adding an auto-dialed participant

If an auto-dialed participant is associated with a template, when the first endpoint connects to the template and establishes a conference, the TelePresence Conductor will ask the conference bridge to dial out to the string that is associated with that auto-dialed participant. This participant will show up as another user in the conference.

Checking cascading

To check that cascading is working properly it is necessary to occupy all the resources on the first conference bridge so that the TelePresence Conductor cascades the conference to the second conference bridge. If there are enough endpoints available you can test this by adding callers to the conference until it is cascaded.

Alternatively, you can increase the number of hosts to reserve resources for on a Lecture-type template to a level that fills the primary conference bridge. This will cause the conference to be cascaded when guests dial in to a conference that is based on that template.

Creating a system backup

To create a backup of TelePresence Conductor system data:

1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file.
   If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format:
   <software version>_<hardware serial number>_<date>_<time>_backup.tar.gz.
   (The file extension is normally **.tar.gz.enc** if an encryption password is specified. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be **.tar.gz.gz** by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)
   The preparation of the system backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
5. Save the file to a designated location.

Log files are not included in the system backup file.

For more information see *Cisco TelePresence Conductor Administrator Guide* or the TelePresence Conductor's online help.

Checking Unified CM message size limit

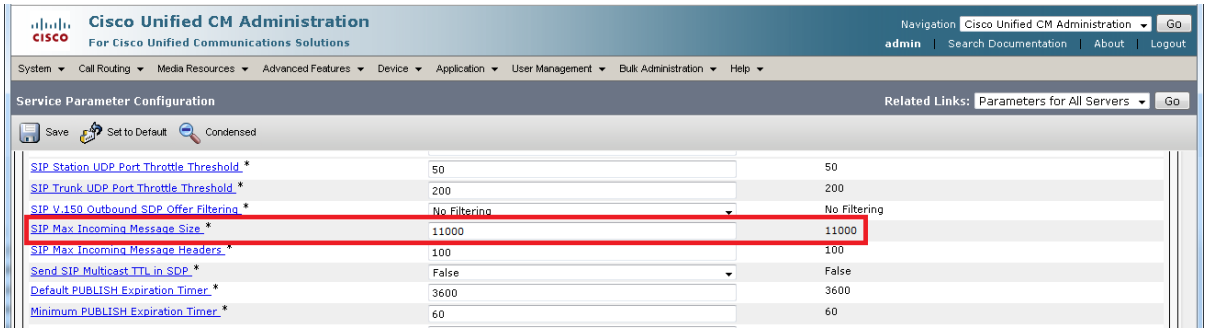
SIP messages for video are considerably larger than SIP messages for audio calls, in particular, when a Cisco TelePresence Server is used in the video network.

Ensure that the **SIP Max Incoming Message Size** on Unified CM is set to 11000:

1. Go to **System > Service Parameters**.
2. Select the appropriate server.
3. Select *Cisco CallManager (Active)* as the service.
4. Select **Advanced**.
5. In the **Clusterwide Parameters (Device – SIP)** configure the field as follows:

SIP Max Incoming Message Size	11000

6. Click **Save**.



Troubleshooting

Viewing logs and calls on TelePresence Conductor

Event log

To see all events associated with a particular conference alias (i.e. across multiple individual conferences) go to **Status > Logs > Event Log > All events** and filter by `Conference_alias_UUID` in the event log either by copying it to the filter box from the event log or by clicking on the hyperlink.

Diagnostic log

Use diagnostic logging (**Maintenance > Diagnostics > Diagnostic logging**) to see the call signaling in the TelePresence Conductor.

Calls/Call history

To see information about currently active calls or a history of calls that have gone through the TelePresence Conductor's back-to-back user agent (B2BUA) go to **Status > Calls > Calls** or **Status > Calls > Call history**.

Viewing route information on Unified CM

Route Plan Report

If the call to the TelePresence Conductor does not get routed, review the route pattern on Unified CM:

1. Go to **Call Routing > Route Plan Report** and click **Find**.
2. Check that the number in **Pattern/Directory Number** is mapped to the correct TelePresence Conductor in **Route Detail**.

Dialed Number Analyzer

If the call to the TelePresence Conductor does not get routed, review the route capability by using the Dialed Number Analyzer (DNA):

1. Go to `https://`<Unified CM `IP Address>/dna` (Note: the DNA service must be activated).
2. Go to **Analysis > Phones** and select the specific SIP UA for verifying the accessibility to conference calls via TelePresence Conductor.
   Note: you can simply run the analyzer without specifying the UA, but results may be general and not include any additional configuration applied on specific UAs.
3. Select the line number on which to run the analysis.
4. Into the **Dialed Digits** field type the digits used in the conference alias.
5. Click **Do Analysis**.

6. **Match Result** should indicate *RouteThisPattern*, if the Unified CM is able to route the incoming call.
7. **Match Result** should indicate *BlockThisPattern*, if the Unified CM is not able to route the incoming call.

Taking a trace on Unified CM using RTMT

RTMT is a tool that lets you monitor system health, view graphs and collect logs from Unified CM. There are versions for both Linux and Windows. Unified CM must also be configured to specify what can be traced.

Configure Unified CM to enable tracing

1. Log in to Unified CM.
2. In the **Navigation** drop-down select **Cisco Unified Serviceability** and click **Go**.
3. Go to the **Troubleshooting Trace Settings** page (**Trace > Troubleshooting Trace Settings**).
4. Select the **Check All Services** check box.
5. Click **Save**.

Installing RTMT – Real Time Monitoring Tool

1. Log in to Unified CM using a Linux or Windows PC.
2. Go to **Application > Plugins**.
3. Select **Find** with 'Name begins with <blank>' and 'Plugin Type equals Installation'.
4. Scroll down to the entry for 'Cisco Unified CM Real-Time Monitoring Tool – Linux' or 'Cisco Unified CM Real-Time Monitoring Tool – Windows', as required.
5. Click on the **Download** link.
6. When downloaded, run the downloaded install file.
7. Follow the instructions in the install wizard.
8. When complete, click **Done** to exit the installer.

Running RTMT

1. Run RTMT. (For example, under windows this is in **Start > All Programs > Cisco > CallManager Serviceability > Real-Time Monitoring Tool**.)
2. In the Login window enter the **Host IP Address**, **User Name** and **Password**.
3. Click **OK**.

Taking a trace using RTMT

1. Select **Trace & Log Central**.
2. Double-click on **Real Time Trace**.
3. Double-click **View Real Time Data**.
4. Select a Node – the Unified CM instance that is to have the trace run on it.
5. Click **Next >**.
6. Select the following:
   - **Products** = *UCM*
   - **Services** = *Cisco CallManager*
   - **Trace File Type** = *sdi*
7. Click **Finish**.

Note:

- Logs can take a while to download.
- The sdi (System Diagnostic Interface) trace contains alarms, error information and SIP stack trace information.

Specific issues

Unable to enable more than one conference bridge

If only a single conference bridge can be enabled, the reason could be that there is no valid release key installed on the TelePresence Conductor.

Contact your Cisco account representative to obtain release key and option keys.

TelePresence Conductor does not communicate with any conference bridges

If the TelePresence Conductor is running without a release key, only a single un-clustered conference bridge is supported.

If the only conference bridge that is enabled on the TelePresence Conductor is clustered, the conference bridge shows as *Unusable* on the **Conference bridge status** page (**Status > Conference bridges**) and the TelePresence Conductor is unable to communicate with any conference bridges.

Contact your Cisco account representative to obtain release key and option keys.

Ad hoc call does not connect

If an ad hoc call fails to connect:

1. If using a TelePresence MCU, go to **Settings > Conferences** and under **Conference Settings** ensure **Media port reservation** is set to *Disabled*.
2. On Unified CM, go to **Media Resources > Conference Bridge** and under the **HTTP Interface Info** section, verify that the **Username**, **Password**, and **HTTP Port** are as configured on the TelePresence Conductor. For Unified CM version 8.6.2, ensure the **HTTP Port** is '80'. If necessary, to reset the password on the TelePresence Conductor go to **Users > Administrator Accounts** and select the account used by Unified CM.
3. On the TelePresence Conductor go to **Users > Administrator accounts**, select the account used by Unified CM and ensure that:
   - **Web access** is *Enabled* (for the purpose of troubleshooting)
   - **API access** is set to *Yes*
   - **State** is *Enabled*

   Ensure that you can log in to the web UI using the Unified CM account credentials.
4. On Unified CM, go to **Media Resources > Conference Bridge** and verify that the conference bridge configured for the TelePresence Conductor is registered to Unified CM.
5. On Unified CM, go to **Media Resources > Conference Bridge** and select the conference bridge. Inside the configuration page verify the IP address used for the conference bridge in Unified CM is the same IP address used for ad hoc calls on the TelePresence Conductor. (On the TelePresence Conductor, go to **Conference configuration > Locations** to see the configured ad hoc IP address).
6. On Unified CM, go to **Media Resources > Media Resource Groups** and verify the Media Bridge Group includes the TelePresence Conductor conference bridge.
7. On Unified CM, go to **System > Location Info > Location** and verify that the locations have enough bandwidth for this call.
8. On the TelePresence Conductor go to **Status > Conference bridge status** to ensure that sufficient resources for all participants in the ad hoc call are available on a single conference bridge. Cascading is not supported in ad hoc conferences, since ad hoc conferences typically comprise of less than five participants and the overhead of cascading such a small conference would be too large.

Rendezvous call does not connect

If a rendezvous call fails to connect:

1. Check, whether your Unified CM is running version 8.6.2 and the endpoint has the ActiveControl feature enabled.
   If Unified CM is running version 8.6.2 and the endpoint has the ActiveControl feature enabled, calls will fail. This is a known limitation, which has been resolved in Unified CM version 9.1.2.
2. On Unified CM, go to **Device > Trunk** and verify that the SIP trunk in Unified CM points to a valid IP address that is configured on TelePresence Conductor under **Conference configuration > Locations**. Check whether you can ping that IP address from other devices.
3. On Unified CM, go to **Call Routing > Route/Hunt > Route Pattern** and verify a route pattern is configured that matches the SIP trunk used to route calls to the TelePresence Conductor. For more information see Task 40: Adding a route pattern to match the SIP trunk connecting to TelePresence Conductor [p.66].
4. On Unified CM, verify the calling privileges, specifically, the Calling Search Spaces (**Call Routing > Class of Control > Calling Search Space**) and Partitions (**Call Routing > Class of Control >Partition**) for that endpoint allow it to make a call.

Conference does not get created

If a conference does not get created, check the list of alarms on the TelePresence Conductor.

If the alarm “Invalid JSON found” has been raised on theTelePresence Conductor and any JSON strings entered into the **Custom parameter** field on the **Advanced template parameters** or **Advanced auto-dialed participant parameters** pages contain double quotes, see Alarm "Invalid JSON found" raised for valid JSON string [p.88].

Auto-dialed participant not connected

If the auto-dialed participant does not get called:

1. On the TelePresence Conductor go to **Conference configuration > Auto-dialed participants** and verify that the settings for the auto-dialed participant are correct, specifically check that:
   - **Participant address** is correct.
   - **Conference name match** will match a valid conference.
   - **State** of the participant is *Enabled*.
2. On the TelePresence Conductor go to **Status > Logs > Event Log > All events** to check whether the TelePresence Conductor tried to call the auto-dialed participant.

3. On the TelePresence Conductor ensure that all conference bridge pools, which can be used by this auto-dialed participant, have a **Location** set. To do this:
   a. Go to **Conference configuration > Auto-dialed participants** and check what the name of the associated conference template is.
   b. Go to **Conference configuration > Conference templates** and check what the name of the associated Service Preference is.
   c. Go to **Conference configuration > Service Preference** and check what the names of the associated Conference bridge pools are.
   d. Go to **Conference configuration > Conference bridge pools**, select each Conference bridge pool identified above and check that it has a Location other than *None* set for the **Location** field.
4. On the TelePresence Conductor go to **Conference configuration > Locations** and verify that
   - the **Conference type** is *Rendezvous*
   - the **SIP trunk settings for out-dial calls** are set correctly to route the auto-dialed participant back to Cisco VCS.
5. On the TelePresence MCU, verify how the conference bridge will dial the auto-dialed participant. Go to **Settings > SIP** and verify that
   - **SIP registrar usage** is *Disabled*
   - **SIP proxy address** is blank
   - **Outgoing transport** is *TLS*
   - **Use local certificate for outgoing connections and registrations** is checked
6. On the TelePresence Server go to **Configuration > SIP Settings** and verify that the **Outbound call configuration** is set to *Call direct*.

Auto-dialed participant disconnected when ad hoc conference is reduced to two parties

The following is a known issue without a workaround.

When an endpoint registered to Unified CM initiates an ad hoc conference, the call is passed to the TelePresence Conductor and any auto-dialed participants associated with the corresponding template are dialed into the conference. When one or more of the endpoints disconnect such that there are only two non-auto-dialed participants connected to the conference, the Unified CM will return the two non-auto-dialed participants to a point-to-point call. The conference will be destroyed and therefore any auto-dialed participants will be disconnected. This will happen whether or not the auto-dialed participant has **Keep conference alive** set to *Yes*.

Guests are disconnected when hosts remain on the cascade MCU only

Guest participants are disconnected from the primary conference bridge even though there are host participants still present on a cascade conference bridge for the same conference. This occurs when:

- The conference bridge type is TelePresence MCU
- The conference template advanced parameter **Disconnect when last host leaves** is set to *true*
- All hosts that were dialed into the primary TelePresence MCU have disconnected
- There are still one or more hosts remaining on a cascade TelePresence MCU
- There are still one or more guests remaining on the primary TelePresence MCU

This issue does not occur on TelePresence Servers, even if the equivalent API parameter `disconnectOnChairExit` has been set to *true* via the custom advanced template parameters.

Conference name displayed on conference bridge is different from conference name that was configured

TelePresence MCUs support conference names of up to 31 characters and TelePresence Servers support conference names of up to 80 characters. If the TelePresence Conductor has a conference name that is longer than the maximum number of supported characters it will hash the name and pass the hash value to the conference bridge for it to use as the conference name. The TelePresence Conductor will continue to use the original name itself.

If a conference name is longer than 31 (for TelePresence MCU) or 80 (for TelePresence Server) characters, you can view the hashed value on the **Conferences status** page (**Status > Conferences**):

- **Name:** shows the conference name used by the TelePresence Conductor
- **Conference name:** shows the hashed value, i.e. the conference name used by the conference bridge.

Duplicate display names

The following is a known issue without a workaround. This will affect both ad hoc and rendezvous conferences.

If three endpoints are in a conference created on the TelePresence Conductor and one of those three endpoints then puts the call on hold and transfers it to a fourth endpoint, the fourth endpoint will appear with the same display name as the endpoint that transferred the call.

Only one screen of a multiscreen endpoint is used

Insufficient configuration

By default, templates on the TelePresence Conductor are configured to provision single-screen systems or the primary screen of multiscreen systems only. If you have a multiscreen endpoint but only the screen related to the main codec is being used in a conference, then ensure that the template being used is set to allow multiscreen systems, as follows:

1. On the TelePresence Conductor, go to **Conference configuration > Conference templates**.
2. Click on the template that is being used for the relevant conference.
3. From the **Allow multiscreen** drop-down menu, select *Yes*.
4. Click **Save**.

If using a Cisco TelePresence System (CTS) endpoint, you must also configure the conference template to use multi-channel audio. If not, insufficient resources will be allocated to the endpoint resulting in only one of the three screens being used.

To provision an endpoint to use multi-channel audio:

1. On the TelePresence Conductor, go to **Conference configuration > Quality settings**.
2. Ensure that there is at least one quality setting with the following configuration:
   - 720p 30fps multi-channel audio, or
   - 720p 60fps multi-channel audio, or
   - 1080p 30fps multi-channel audio.

   If not, create a new quality setting by clicking **New**.
3. Go to **Conference configuration > Conference templates**.
4. Click on the template that is being used for the relevant conference.
5. From the **Participant quality** drop-down menu (for Meetings), or either the **Host quality** or **Guest quality** drop-down menu (for Lectures), select the appropriate multi-channel audio quality setting.
6. Click **Save**.

Cascaded conferences

Only single screen endpoints are supported on cascade links connecting TelePresence Servers. Therefore, if a multiscreen endpoint joins a conference on a cascade conference bridge, participants on the same cascade bridge will see all screens, whereas participants on the primary bridge and on other cascade bridges will only see one screen (the screen showing the loudest speaker).

CTS endpoint cannot join a conference on a TelePresence Server

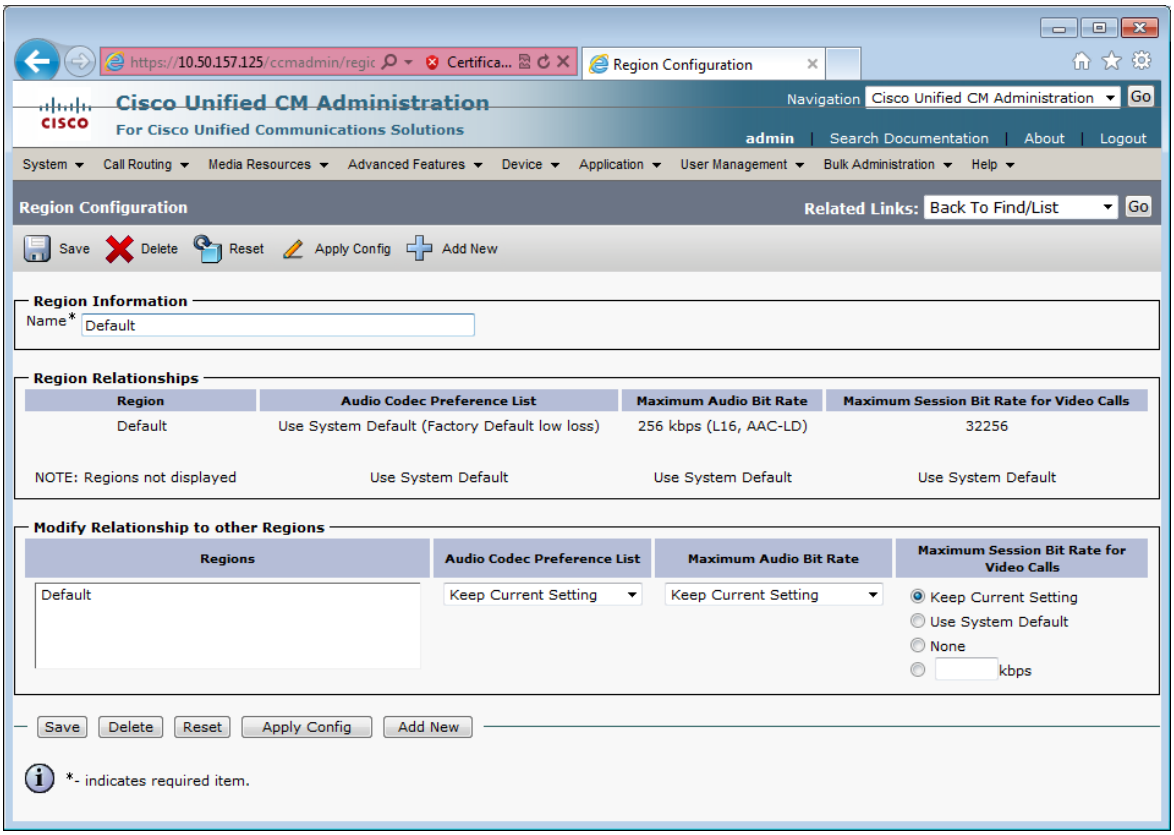
If your deployment includes one or more CTS endpoints and TelePresence Servers, the CTS may not be able to join or create conferences hosted on the TelePresence Server. In such cases calls will be rejected with a **Media Negotiation Failure**.

To resolve this issue on Unified CM version 8.6.2:

1. Log in as a user with administrator privileges.
2. Navigate to **System > Region**.
3. For each region that includes the CTS, ensure that the settings are:
   - Max Audio Bit Rate: 256 kbps (L16, AAC-LD).
   - Max Video Call Bit Rate (Includes Audio): 32256.

To resolve this issue on Unified CM 9.0 and later:

1. Log in as a user with administrator privileges.
2. Navigate to **System > Region information > Region**.
3. For each region that includes the CTS, ensure that the settings are:
   - Maximum Audio Bit Rate: 256 kbps (L16, AAC-LD).
   - Maximum Session Bit Rate for Video Calls: 32256.



Pre-configured endpoint cannot join conference

When you pre-configure single-screen and multiscreen endpoints on the TelePresence Conductor, you specify the address of each codec used by the endpoint.

In certain scenarios the address of the endpoint may change depending on where it registers to (for example if the domain portion of the URI is the IP address of the peer the endpoint is registering to). If not all addresses that the endpoint can be known as are listed in the pre-configured endpoints configuration in TelePresence Conductor, the TelePresence Conductor may not recognize its address and the endpoint will use the template default settings rather than the known endpoint settings.

To resolve this, you must ensure that all possible addresses that could be used by the codec are listed.

To do this:

1. On the TelePresence Conductor, go to **Conference configuration > Pre-configured endpoints**.
2. From the list of pre-configured endpoints select the endpoint in question.
3. In the **Codecs** section at the bottom of the page, click on the first codec.
4. In the **Optional address** fields, ensure that all possible addresses from which calls for this codec could be received are listed.

5. Click **Save**.
6. Repeat steps 3-5 for each codec configured for that endpoint.

ActiveControl does not work on one or more endpoint(s)

If Unified CM is running versions 9.0 or 9.1 the ActiveControl feature does not work on endpoints registered to this Unified CM. This is a known limitation, which has been resolved in Unified CM version 9.1.2.

The iX Protocol must be enabled in the advanced template parameters of the TelePresence Conductor. See **Configuring ActiveControl and iX protocol** in *Cisco Collaboration Meeting Rooms (CMR) Premises Deployment Guide* for more information.

Alarm "Invalid JSON found" raised for valid JSON string

It may be possible for the alarm “Invalid JSON found” to be raised even though the JSON string that was entered into the **Custom parameter** field on the **Advanced template parameters** or **Advanced auto-dialed participant parameters** pages appears to have been entered correctly. The alarm is raised if the JSON string contains double quotes (“) with the Unicode value of 147 instead of the Unicode value 34. The Unicode value 147 is used in some external editors from which you may have copied the JSON string.

Sending the JSON string with the unsupported double quotes to the conference bridge will prevent the conference from being created.

To work around this issue, re-type the double quotes contained in the JSON string within the user interface field.

Error messages

Error communicating with mcu error="Method not supported" – this may be because a physical TelePresence Server has been added as a TelePresence MCU bridge or the slave conference bridge of a cluster has been configured.

Unsupported conference bridge software version - this may be because a physical TelePresence MCU has been added as a TelePresence Server bridge.

Regular expression match and replace

A regular expression replace of \12\2 will replace with 12th bracket match and follow it with the 2nd bracket match.

If a match of the 1st bracket match, followed by the insertion of the literal digit 2 followed by the 2nd bracket match is required, then named matches need to be used. These work as follows:

(?P<id>123)456(789) will store

123 as **\1**

789 as **\2**

123 as named replace: **<id>** (the name used inside the "<" and ">" is user selectable)

to replace, use:

\g<id>

so to replace the 1st bracket match, followed by the insertion of the literal digit 2 followed by the 2nd bracket match use:

\g<id>2\2

Appendix 1: Unified CM version 8.6.2 configuration

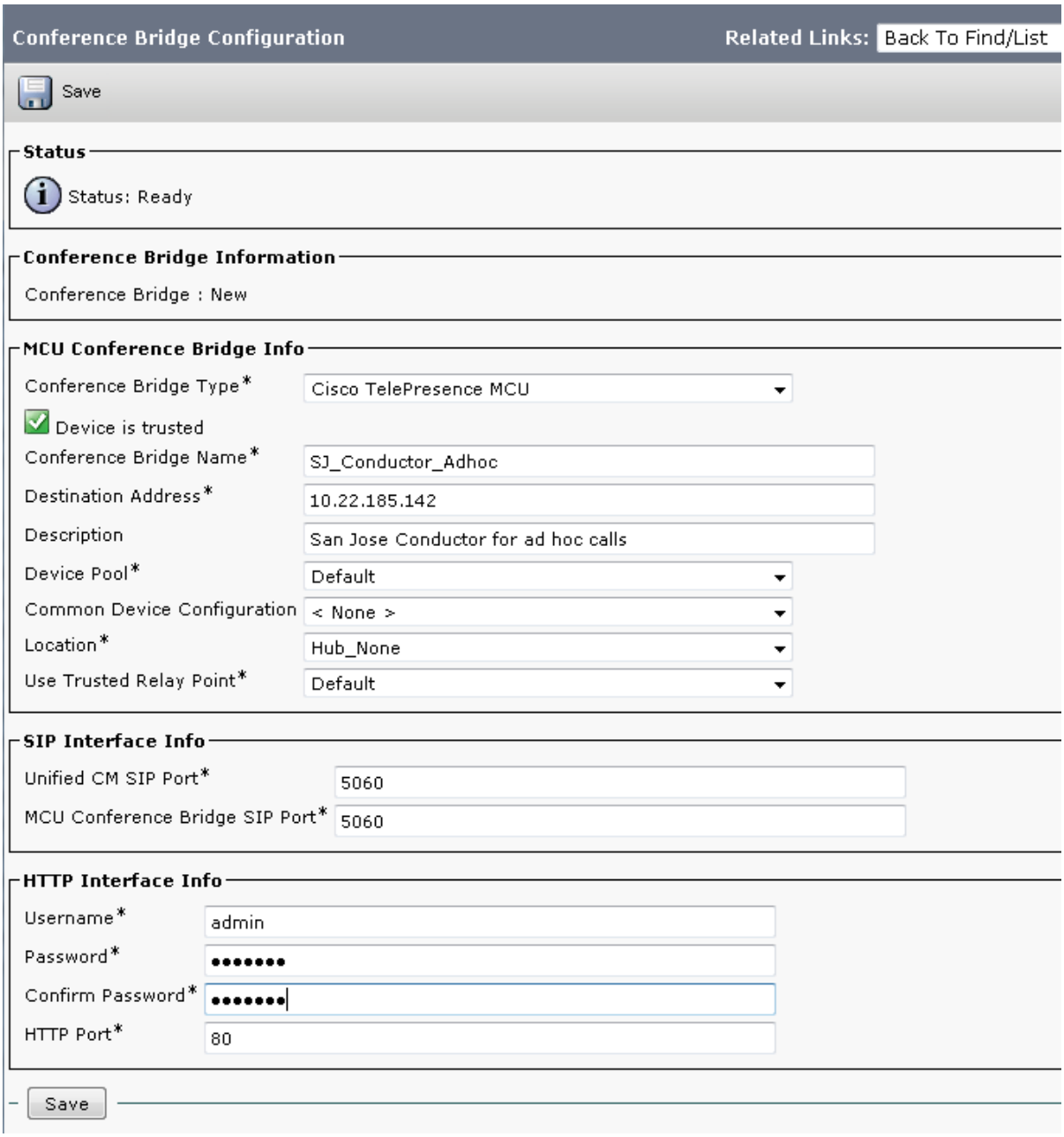
This section covers the differences between version 8.6.2 and version 10.x of Unified CM when configuring it for use with the TelePresence Conductor. The individual steps in the section Configuring Unified CM [p.50] are from a Unified CM version 10.x and should be replaced with the relevant steps from this appendix for Unified CM version 8.6.2 configuration.

Adding TelePresence Conductor to Unified CM for ad hoc conferences

For Unified CM version 8.6.2, replace Task 35: Adding the TelePresence Conductor as a Conference bridge to Unified CM [p.57] with the following:

1. Go to the Unified CM web interface and log in as an admin user.
2. Go to **Media Resources > Conference Bridge**.
3. Click **Add New** to create a new conference bridge.
4. Enter the following into the relevant fields, leave other fields as their default values:

Conference Bridge Type	Select *Cisco TelePresence MCU*.
Conference Bridge Name	Enter the TelePresence Conductor's name.
Destination Address	Enter the TelePresence Conductor's location-specific ad hoc IP address.
Device Pool	Select the appropriate Unified CM Device pool.
Location	Select the appropriate Unified CM Location.
Username	Enter the username of the TelePresence Conductor administration user set up earlier. This appears on the TelePresence Conductor's **Administrator accounts** page (**Users > Administrator accounts**).
Password	Enter the password of the TelePresence Conductor administration user.
HTTP Port	Enter ‘80’.



5. Click **Save**.
6. Click **Reset** for the changes to take effect.
7. Find the **Related Links: Back to Find/List** and click **Go**.
8. Verify that the TelePresence Conductor is registered with Unified CM:

Appendix 2: Unified CM version 9.x configuration

This section covers the differences between version 9.x and version 10.x of Unified CM when configuring it for use with the TelePresence Conductor. The individual steps in the section Configuring Unified CM [p.50] are from a Unified CM version 10.x and should be replaced with the relevant steps from this appendix for Unified CM version 9.x configuration.

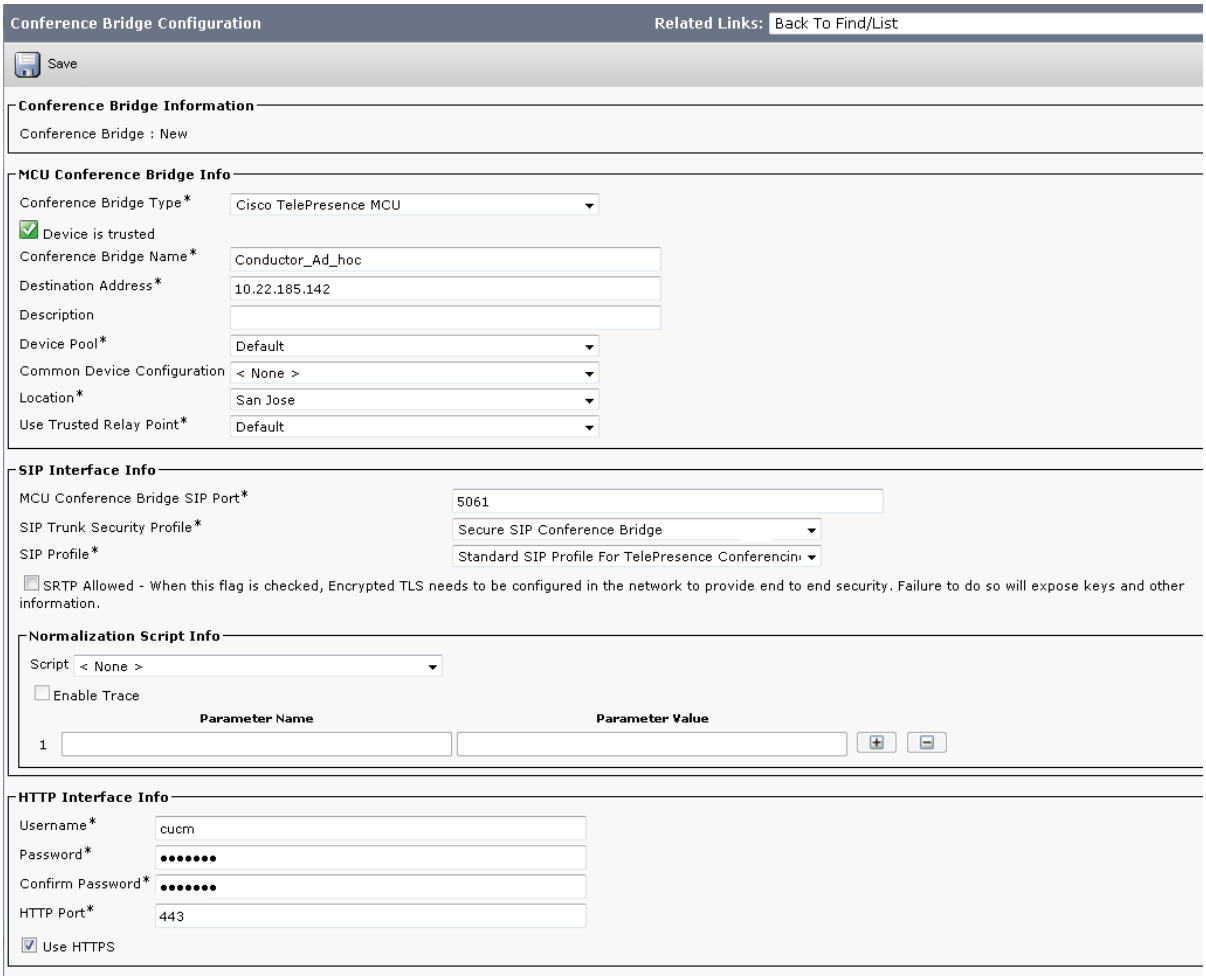
Adding TelePresence Conductor to Unified CM for ad hoc conferences

For Unified CM version 9.x, replace Task 35: Adding the TelePresence Conductor as a Conference bridge to Unified CM [p.57] with the following:

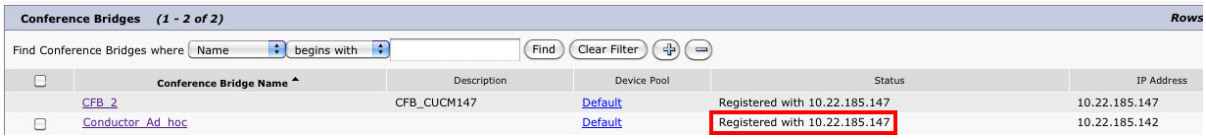
1. Go to the Unified CM web interface and log in as an admin user.
2. Go to **Media Resources > Conference Bridge**.
3. Click **Add New** to create a new conference bridge.
4. Enter the following into the relevant fields, leave other fields as their default values:

Conference Bridge Type	Select *Cisco TelePresence MCU*.
Conference Bridge Name	Enter the TelePresence Conductor's name.
Destination Address	Enter the TelePresence Conductor's location specific ad hoc IP address.
Device Pool	Select the appropriate Unified CM Device pool.
MCU Conference bridge SIP Port	Check the SIP listening port, leave it as default, or change it as appropriate for your design.
SIP Trunk Security Profile	Select *Secure SIP Conference Bridge*.
SIP Profile	Select *Standard SIP Profile for TelePresence Conferencing*.
Location	Select the appropriate Unified CM location.
Username	Enter the username of the TelePresence Conductor administration user set up earlier. This appears on the TelePresence Conductor's **Administrator accounts** page (**Users > Administrator accounts**).
Password	Enter the password of the TelePresence Conductor administration user.
HTTP Port	Enter '443'.

Use HTTPS	Tick this box.



5. Click **Save**.
6. Find the **Related Links: Back to Find/List** and click **Go**.
7. Verify that the TelePresence Conductor is registered with Unified CM.



Appendix 3: Adding the Unified CM normalization script

If your deployment uses encryption and TLS on a SIP trunk between Unified CM and TelePresence Conductor, you must add the normalization script to Unified CM. To do this:

1. Download the script from the Cisco website.

   Note: it is fine to use the Unified CM version 9.1 normalization script until the Unified CM version 10.x normalization script is available.
2. On Unified CM, go to **Device > Device Settings > SIP Normalization Script**.
3. Click **Add new**.
4. Click **Import File**.
5. Select the script that you downloaded.
6. Click **Import File**.
7. Enter or change the following details:

Name	Enter `telepresence-conductor-interop`.
Description	Enter `Provides interoperability for calls through the TelePresence Conductor`.
Memory Threshold	Enter '1000'.
Lua Instruction Threshold	Enter '2000'.

8. Click **Save**.
9. For rendezvous conferences, for all Unified CM versions:
   a. Go to **Device > Trunk** and select the SIP trunk used for rendezvous conferences.
   b. In the **Normalization script** section, within the **SIP Information** section, towards the bottom of the page, from the drop-down list select the script you have just added (**telepresence-conductor-interop**).
   c. Click **Save**.
   d. Click **Reset**.
10. For ad hoc conferences, for Unified CM versions below 10.x:
    a. Go to **Media Resources > Conference Bridge** and select the conference bridge used for ad hoc conferences.
    b. In the **Normalization Script Info** section, within the **SIP Information** section, towards the bottom of the page, from the drop-down list select the script you have just added (**telepresence-conductor-interop**).

c. Click **Save**.

d. Click **Reset**.

11. For ad hoc conferences, for Unified CM versions 10.x or later:

a. Go to **Device > Trunk** and select the SIP trunk used for ad hoc conferences.

b. In the **Normalization script** section, within the **SIP Information** section, towards the bottom of the page, from the drop-down list select the script you have just added (**telepresence-conductor-interop**).

c. Click **Save**.

d. Click **Reset**.

Appendix 4: Ensuring that Unified CM trusts TelePresence Conductor's server certificate and vice versa

For Unified CM and TelePresence Conductor to establish a TLS connection with each other, the following tasks are required.

Loading server and trust certificates on TelePresence Conductor

TelePresence Conductor server certificate

TelePresence Conductor has only one server certificate. By default, this is a certificate signed by a temporary certificate authority. We recommend that it is replaced by a certificate generated by a trusted certificate authority.

For information on how to request a certificate see *Cisco TelePresence Conductor Certificate Deployment Guide*.

To upload a server certificate:

1. Go to **Maintenance > Security certificates > Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.
3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the TelePresence Conductor was used to produce the CSR for this server certificate.)
   - The **server private key** PEM file must not be password protected.
   - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data**.

Note: If you are using Unified CM version 8.5(1) or earlier and are having problems establishing a TLS connection between TelePresence Conductor and Unified CM, we recommend adding the following x509 extended key attributes into the CSR:

- serverAuth (1.3.6.1.5.5.7.3.1) -- TLS Web server authentication
- clientAuth (1.3.6.1.5.5.7.3.2) -- TLS Web client authentication
- ipsecEndSystem (1.3.6.1.5.5.7.3.5) -- IP security end system

TelePresence Conductor trusted CA certificate

The **Trusted CA certificate** page (**Maintenance > Security certificates > Trusted CA certificate**) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this TelePresence Conductor. When a TLS connection to TelePresence Conductor mandates certificate verification, the certificate presented to the TelePresence Conductor must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

The root CA of the Unified CM server certificate must be loaded into the TelePresence Conductor's trusted CA certificate list.

To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.

Repeat this process on every TelePresence Conductor that will communicate with this Unified CM (if using a TelePresence Conductor cluster).

Loading server and trust certificates on Unified CM

Certificate management for Unified CM is performed in the **Cisco Unified OS Administration** application.

All existing certificates are listed under **Security > Certificate Management**. Server certificates are of type *certs* and trusted CA certificates are of type *trust-certs*.

Unified CM server certificate

By default, Unified CM has a self-signed server certificate **CallManager.pem** installed. We recommend that this is replaced with a certificate generated from a trusted certificate authority.

Unified CM trusted CA certificate

To load the root CA certificate of the authority that issued the TelePresence Conductor certificate (if it is not already loaded):

1. Click **Upload Certificate/Certificate chain**.
2. Select a **Certificate Name** of *CallManager-trust*.
3. Click **Browse** and select the file containing the root CA certificate of the authority that issued the TelePresence Conductor certificate.
4. Click **Upload File**.

Repeat this process on every Unified CM server that will communicate with TelePresence Conductor. Typically this is every node that is running the CallManager service.

Appendix 5: Resilient deployment using clustered TelePresence Conductors

As part of a solid network design, resiliency of the conferencing system is critical. This can be achieved for a TelePresence Conductor integration using a second and even third TelePresence Conductor cluster peer and two or more conference bridges per location.

For further details on how to configure a cluster of TelePresence Conductors, see *Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide*.

Appendix 6: Multiparty Licensing

Multiparty Licensing lets you administer licenses centrally on the Cisco TelePresence Conductor instead of loading screen licenses locally onto the Cisco TelePresence Servers. Compared to traditional screen licensing, Multiparty Licensing allows for greater capacity at lower cost. Two variants are available:

- Personal Multiparty (PMP) licenses. Each license is assigned to a specific user. PMP licenses are suitable for users who initiate conferences frequently.
  PMP licenses are purchased through Cisco Unified Workspace Licensing (CUWL Pro). They are available for deployments with Unified CM for call control.
- Shared Multiparty (SMP) licenses. Each license is shared by multiple users, but only in one conference at a time. SMP licenses are suitable for users who initiate conferences infrequently.
  SMP licenses are available for deployments with either Unified CM or Cisco VCS for call control.

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

Limitations

- Unified CM-based deployments—Cisco VCS-based deployments are not supported.
- TelePresence Server-hosted conferences—TelePresence MCUs are not supported.

Feature support

Table 1: Multiparty Licensing Features

Feature	Supported?
Collaboration Meeting Rooms provisioned by Cisco TMSPE/Rendezvous conferences in TelePresence Conductor	Yes
Ad hoc escalated conferences	Yes
TelePresence Conductor scheduling in Cisco TMS	Yes. Conductor API allows TMS to schedule meetings by specifying the `external_owner_id`.
Maximum conference size	Limited by the conference bridge capacity, concurrent usage, and the deployment's total number of Screen licenses included in license packs.
Number of concurrent conferences per named host	1

Table 1: Multiparty Licensing Features (continued)

Feature	Supported?
Requirement that host is present in the conference	Yes
Maximum video resolution	Limited only by conference bridge capabilities
Maximum content quality	Limited only by conference bridge capabilities
Multiscreen support	Yes

Personal Multiparty

Personal Multiparty provides a license for a named user to host a video conference with as many participants as the conference bridge resources allow.

Configuration requirements

- The number of conference aliases must not exceed the number of licenses.

Configuration tasks

Ad hoc conferences

Follow the tasks in the main body of this deployment guide to configure the TelePresence Conductor to work with Unified CM and a pool of conference bridges for ad hoc conferences.

- The conference bridges must be of type TelePresence Server.
- In Configuring the TelePresence Conductor [p.26] you can specify a Personal Multiparty conference template with settings that are suitable to your deployment.
- In Task 21: Creating an ad hoc Location [p.38] the conference template must be the Personal Multiparty conference template created in the previous task.

Rendezvous/personal CMR conferences

For rendezvous/personal CMR conferences we highly recommend that you create a CMR via Cisco TMSPE. To do this:

1. Follow the instructions up to and including Task 18: Adding IP addresses for ad hoc and rendezvous locations on TelePresence Conductor [p.35] in this deployment guide.
2. Follow the instructions in the *Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide* to provision a CMR for Personal Multiparty.

Alternatively, if you would like to configure a rendezvous conference via the TelePresence Conductor user interface:

1. Follow the instructions applicable to rendezvous conferences in this deployment guide.
2. Instead of Configuring the TelePresence Conductor [p.26] add conference aliases for the named hosts. The aliases must not contain regular expressions. They should use a format such as **<named_host>@<domain>**.

Tracking the number of licenses used

In order to comply with EULA terms, the administrator must ensure that the number of CMRs/rendezvous conferences created does not exceed the number of licenses purchased.

For detail on license terms and acquiring an overview of available licenses, see the Cisco Collaboration Meeting Rooms (CMR) Premises web page.

If you have configured CMRs follow the instructions in the section **Tracking the number of licenses used** in *Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide*.

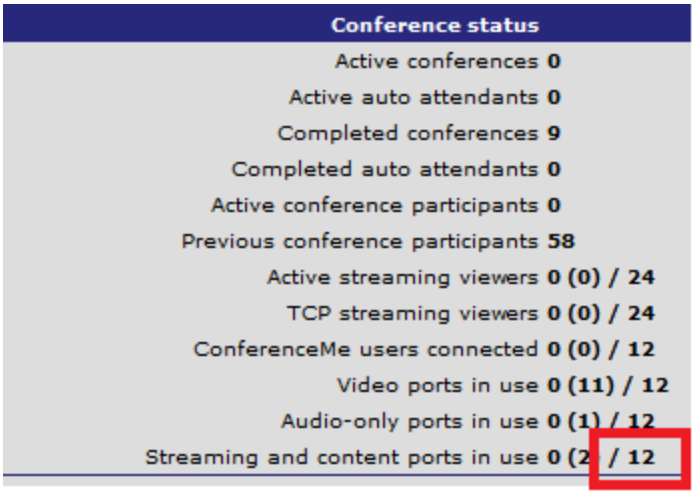
If you have configured conference aliases on the TelePresence Conductor user interface:

1. Go to **Conference configuration > Conference templates**
2. Select the conference template for Personal Multiparty conferences.
3. Verify the number of aliases listed under **Aliases associated with this template**.

Appendix 7: Identifying dedicated content ports on a Cisco TelePresence MCU

This information is available on the spec sheet for the TelePresence MCU, but it is also available through the web interface, the steps below describe how to locate and use this information.

1. Go to the TelePresence MCU in a browser.
2. Log in as administrator.
3. Go to **Status > Conferences** and look at the line marked **Streaming and content ports in use 0 (0)/##**, where ## is the number of dedicated content ports of this TelePresence MCU.



Document revision history

The following table summarizes the changes that have been applied to this document:

Date	Description
June 2015	Updated for release XC4.0
February 2015	Added a task on adding ad hoc IP address(es) to the server certificate SAN list
January 2015	Added section on checking the Unified CM message size limit
January 2015	Updated for release XC3.0
November 2014	Added appendix on Personal Multiparty.
September 2014	Updated for release XC2.4
July 2014	Corrected a hyperlink and changed some wording to be clearer.
April 2014	Updated for release XC2.3
March 2014	Removed configuration task on Unified CM within Personal 4-Way Multiparty Conferencing section.
February 2014	Added appendix for Personal 4-Way Multiparty Conferencing and corrected link to UCM normalization script.
August 2013	Updated for release XC2.2
August 2013	Corrected the recommendation for uploading server certificates and how to troubleshoot auto-dialed participants not being called
May 2013	Updated for release XC2.1
April 2013	Corrected the SIP configuration for MCUs
March 2013	Added information about lack of cascading support in ad hoc conferences
February 2013	Restructured the document and updated some screen shots
December 2012	Initial release.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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

© 2015 Cisco Systems, Inc. All rights reserved.