Cisco TelePresence Conductor with Cisco Unified Communications Manager

Deployment Guide

XC2.2

Unified CM 8.6.2 and 9.x

D14998.09

Revised March 2014

Contents

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.

Further reading

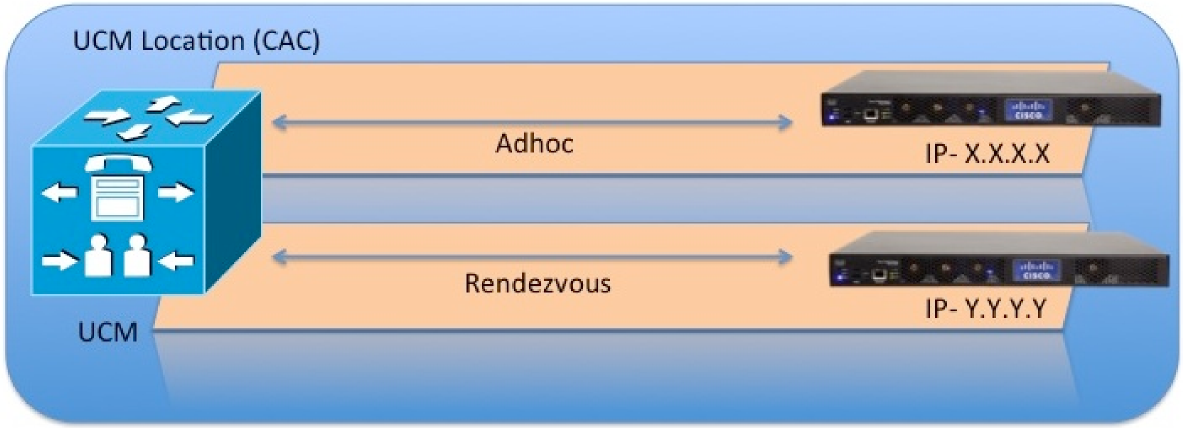
This document focuses on the key components needed for a Unified CM and TelePresence Conductor integration only. For more details on how to implement a Unified CM or Unified CM cluster reference the Cisco Unified Communications Manager documentation on www.cisco.com.

For details on how to deploy a cluster of TelePresence Conductor with Unified CM please see *Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide* (D14828).

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* (D14827) or *Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide* (D15014) depending on the type of Cisco VCS deployment.

About Cisco TelePresence Conductor and Cisco Unified Communications Manager

In the 8.6.2 version of Unified CM software, 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.

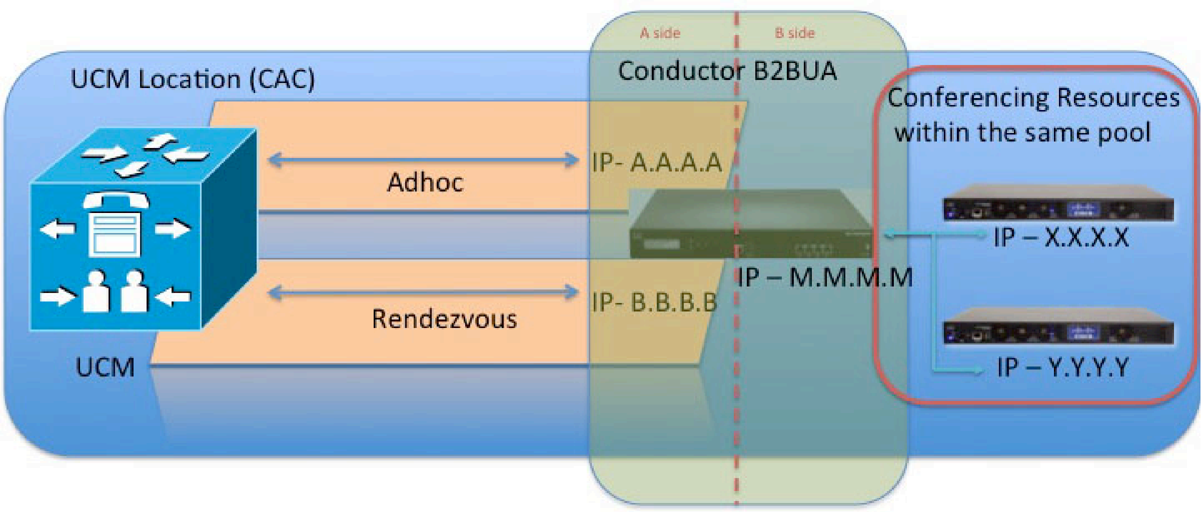


TelePresence Conductor version XC2.2 can be configured to emulate conference bridges for Unified CM; using its back-to-back user agent (B2BUA) it can route the different types of conference call (ad hoc or rendezvous) to one or more conference bridges. These bridges can be Cisco TelePresence MCUs or Cisco TelePresence Servers.

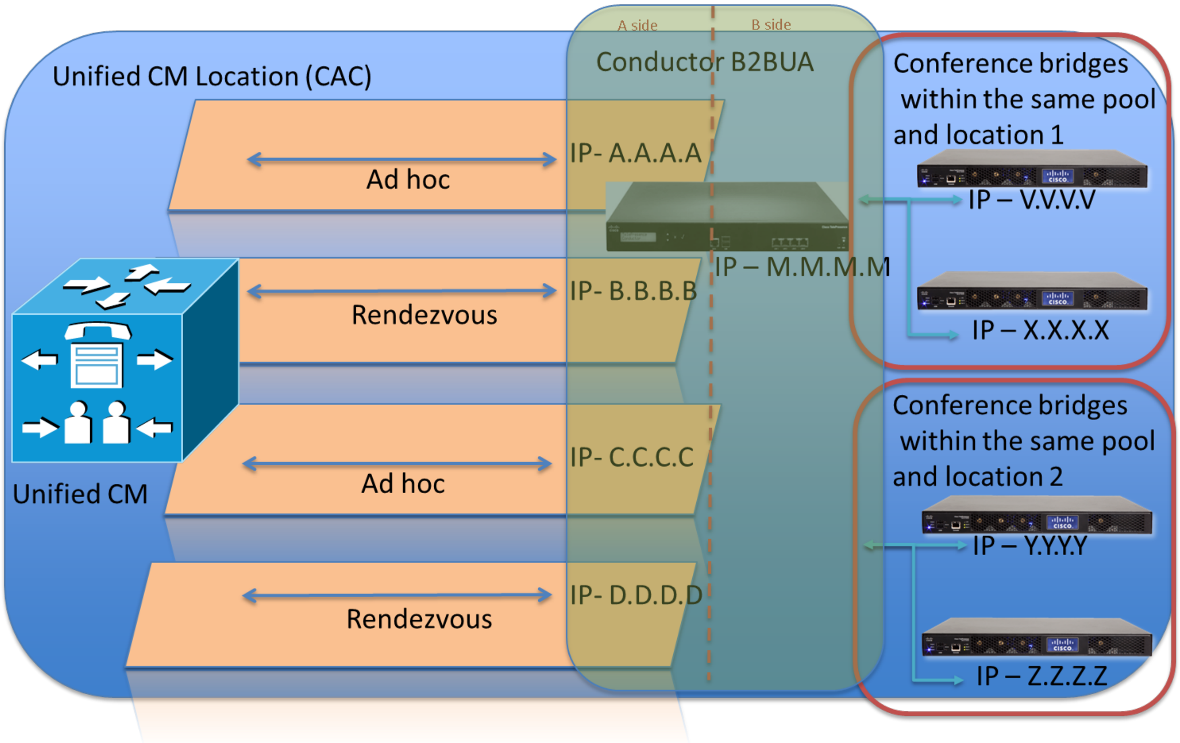
Without the TelePresence Conductor, Unified CM has to be configured to connect directly to the video multipoint control unit bridging resources – separate conference bridges are required for ad hoc conferences and rendezvous conferences.

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

Note: For ad hoc conferences the conference bridges to use are indirectly configured 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 XML RPC and SIP messaging is used. The destination for both these 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, the MRG to an MRGL, then the MRGL to a Device, either directly or by assigning the MRGL for use by a Device pool

For rendezvous conferences a 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.

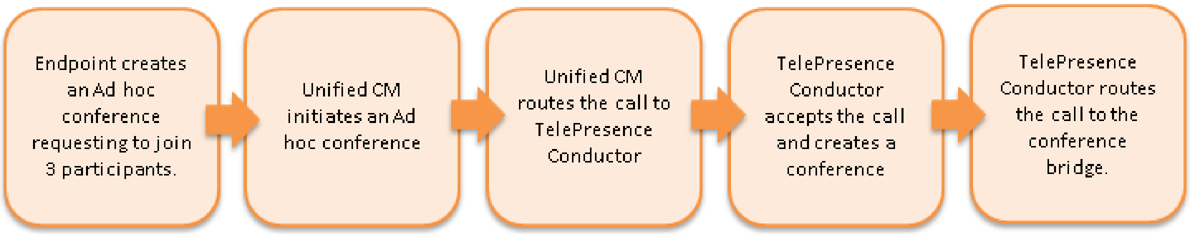
For out-dialed calls from TelePresence Conductor to Unified CM TelePresence Conductor will use the reverse path of the SIP Trunk used for rendezvous calls.

Call flow with the TelePresence Conductor

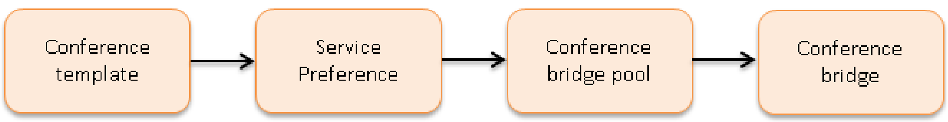
The following sections show the call flows that occur when handling ad hoc and rendezvous calls.

Ad hoc call flow

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



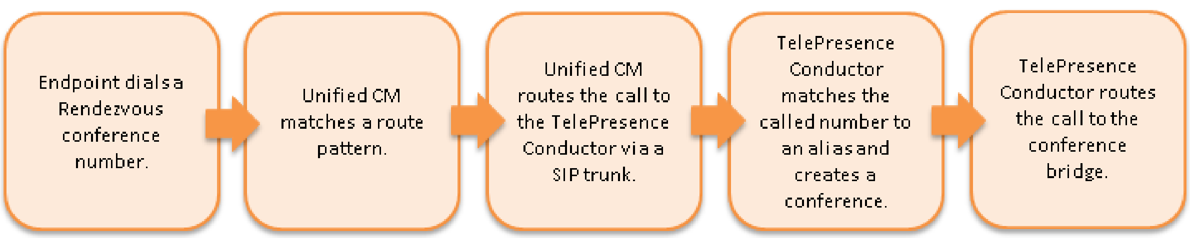
In TelePresence Conductor:



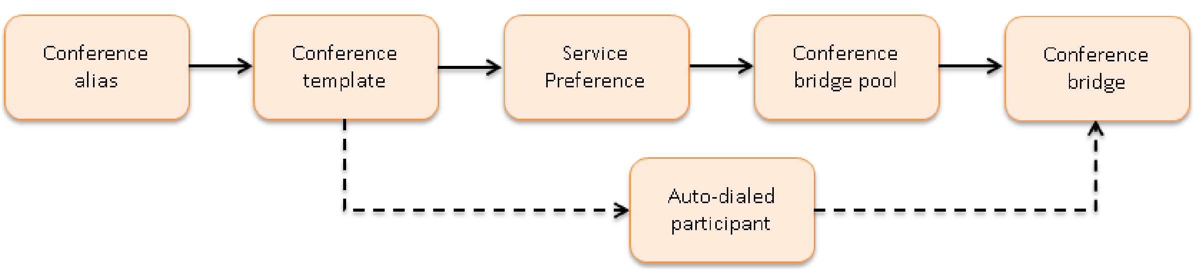
Once these parts of the call flow are complete, the calls are set up and media flows between the endpoint and the conference bridge.

Rendezvous call flow

This diagram shows the call flow for a rendezvous call:



In TelePresence Conductor:

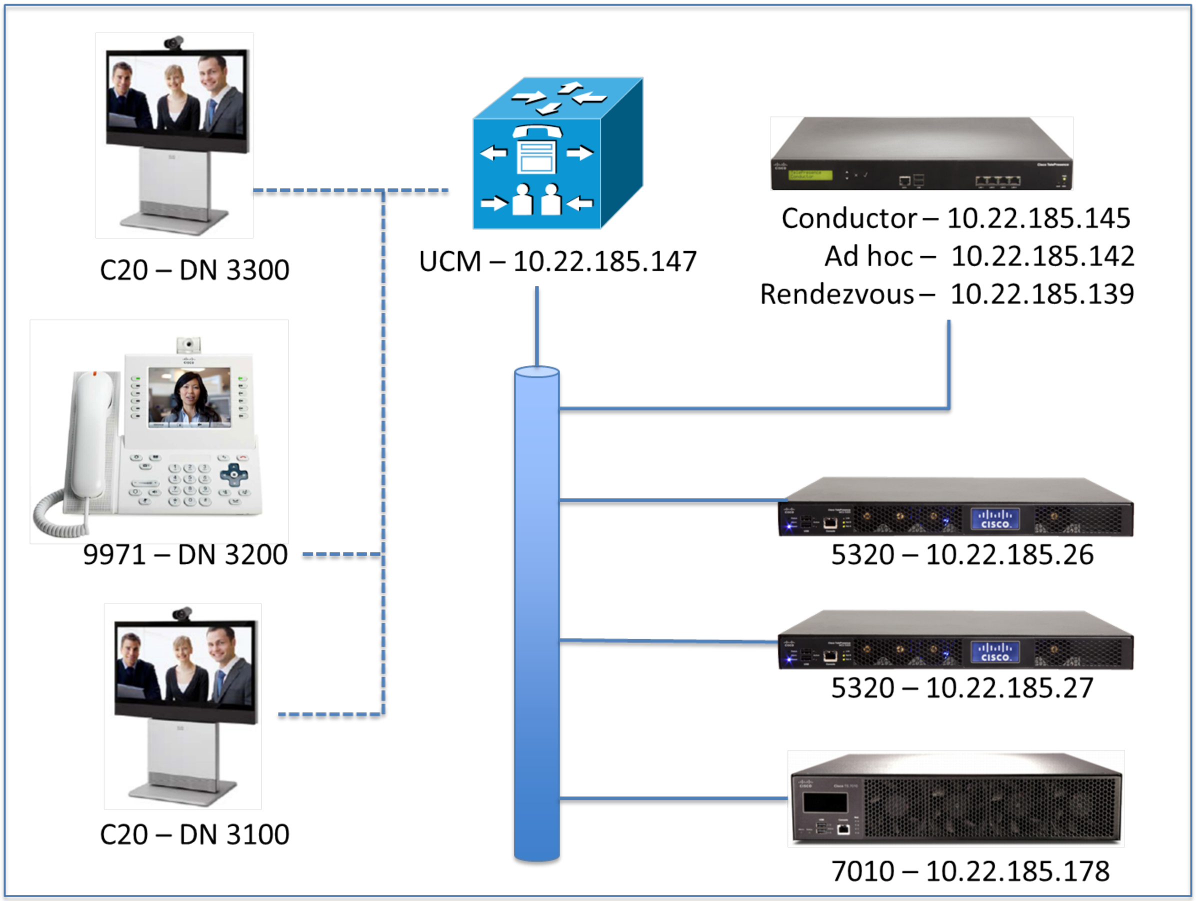


(The dotted line indicates an optional step where auto dialled participant(s) are configured on the TelePresence Conductor for the relevant template.)

Once these parts of the call flow are complete then the call is set up and media flows between the endpoint 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 XC2.2 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 9971 and EX90, or room systems such as the MX300.

Deploying TelePresence Conductor with Unified CM

Prerequisites

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

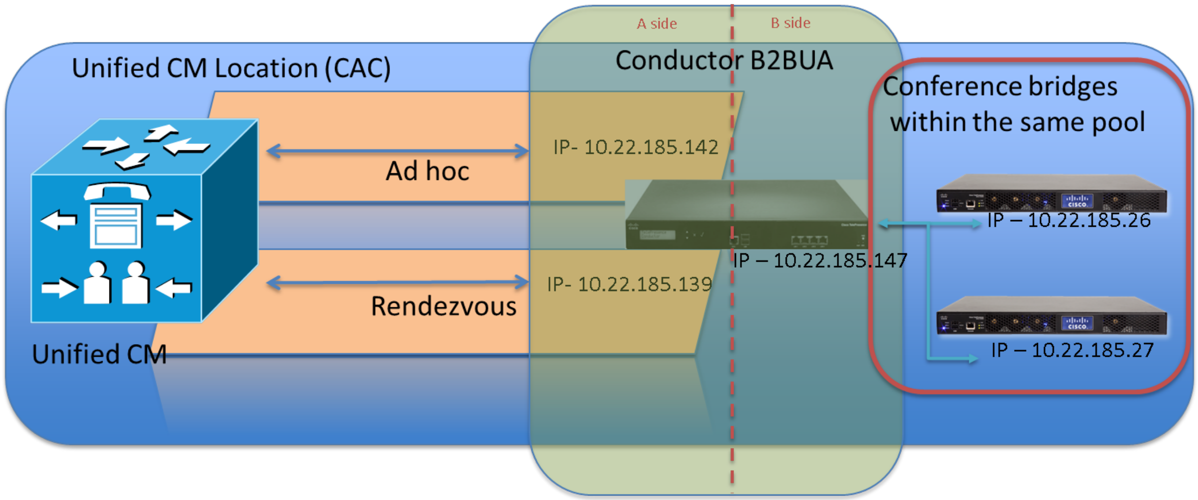
- The Unified CM must already be configured with a base configuration and must be running Unified CM version 8.6.2 or later. We highly recommend that you use version 9.1.1 to support encryption of rendezvous and ad hoc calls using SRTP and SIP TLS.
  Ensure connectivity by registering at least three 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 XC2.2 and accessible over the network. For assistance in reaching this stage see *Cisco TelePresence Conductor Getting Started 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.
- 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 software version 4.4 or later, 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 software version 3.1 or later, otherwise some features will not be supported.
- 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, e.g. TE6.0 or higher.
- A web browser is available with access to the web interfaces of the Unified CM, TelePresence Conductor and conference bridges that are being configured.

Integration overview

The configuration below is based on the Example network deployment [p.9] shown below:



Note: the configuration shows how to configure both TelePresence MCUs and TelePresence Servers for use in this configuration. It is not necessary to configure both types; if you only have one type, follow the instructions for configuring that one and ignore the instructions for the conference bridge that you do not have.

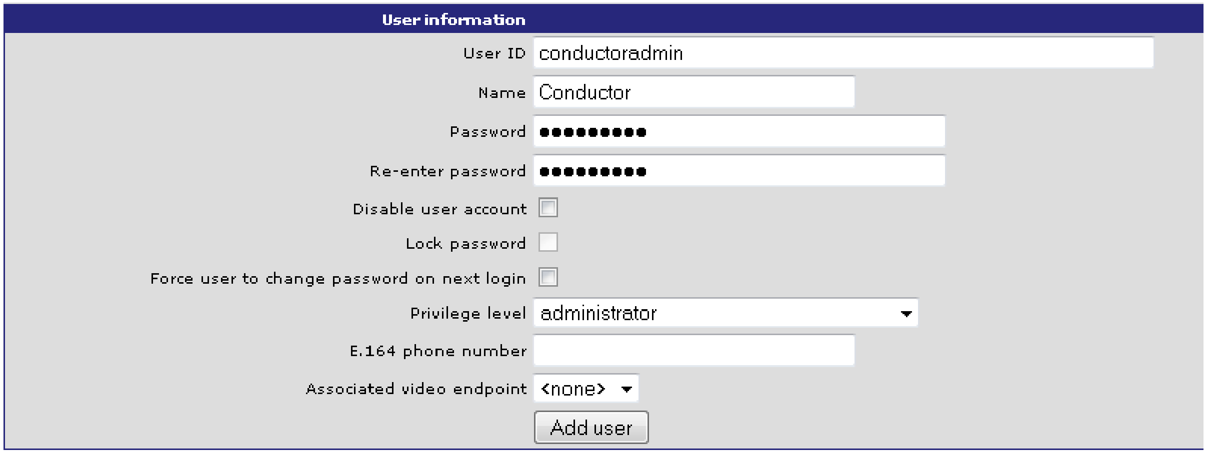
Configuring the TelePresence MCU

Task 1: 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. Go to the web interface of the TelePresence MCU you want to configure and log in as an administrator.
2. Go to **Users** and click **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.
Force user to change password on next login	Uncheck.
Privilege level	Select *administrator*.



4. Click **Add user**.
5. Repeat the steps for any other TelePresence MCUs.

Task 2: 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:

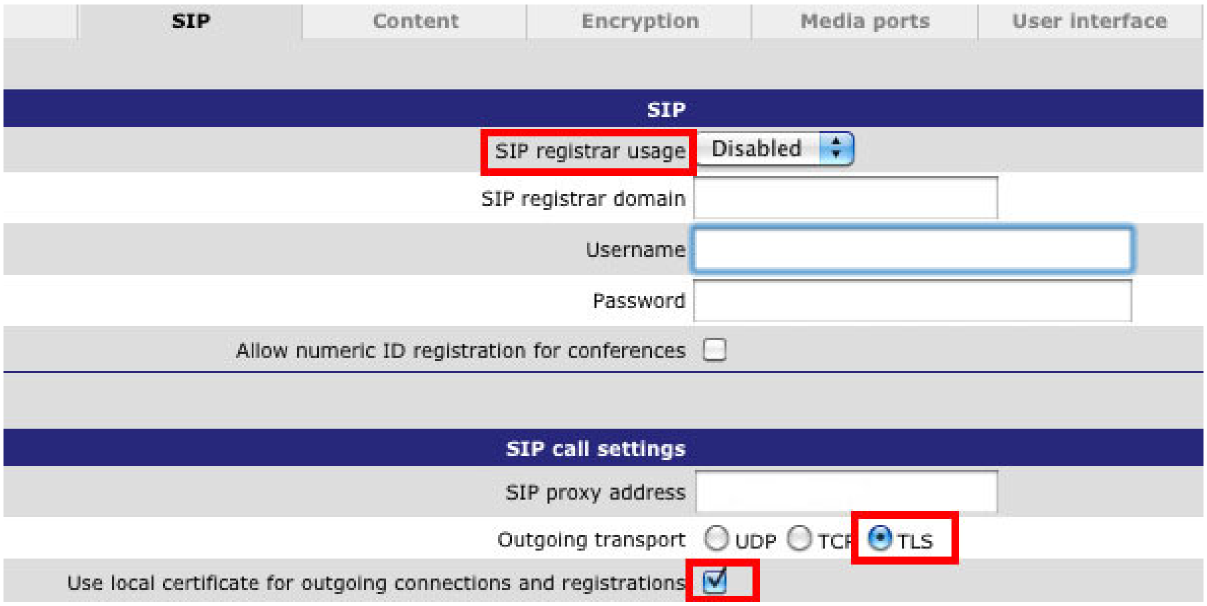
1. Go to **Settings > Encryption**.
2. Set **Encryption status** to *Enabled*.
3. Set **SRTP encryption** to *Secure transport (TLS) only*.
4. Click **Apply changes**.
5. Go to **Network > Services**.
6. Ensure that **HTTPS (port 443)** is checked.
7. Ensure that **Encrypted SIP (TLS)** is checked.
8. Ensure that **SIP (UDP)** is unchecked.
9. Click **Apply changes**.

Task 3: 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*.
SIP proxy address	Leave blank.

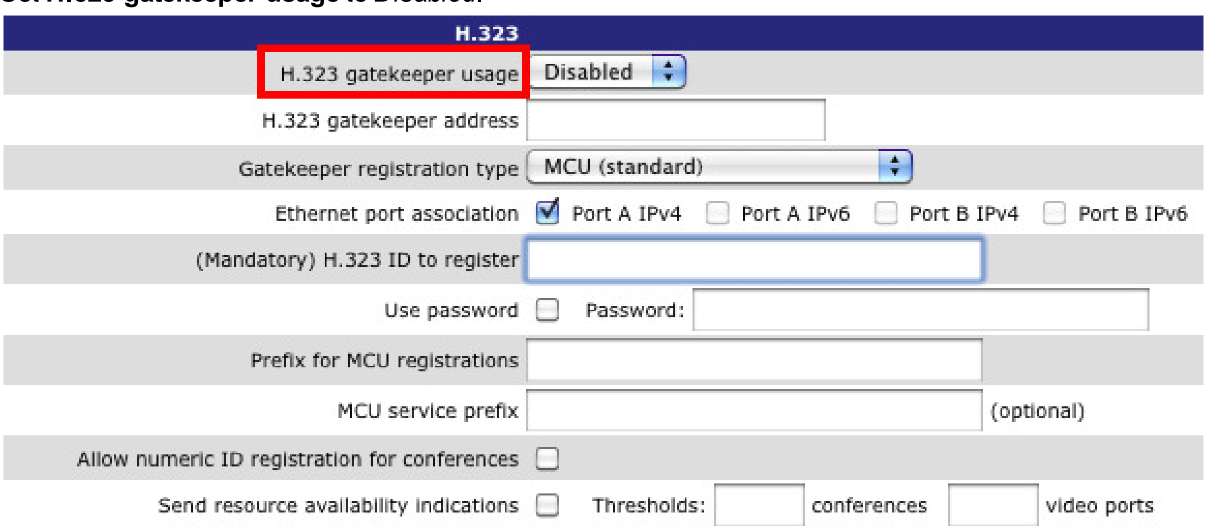
Outgoing transport	Select *TLS*.
Use local certificate for outgoing connections and registrations	Check the box.



3. Click **Apply changes**.

Task 4: Disabling H.323 registration

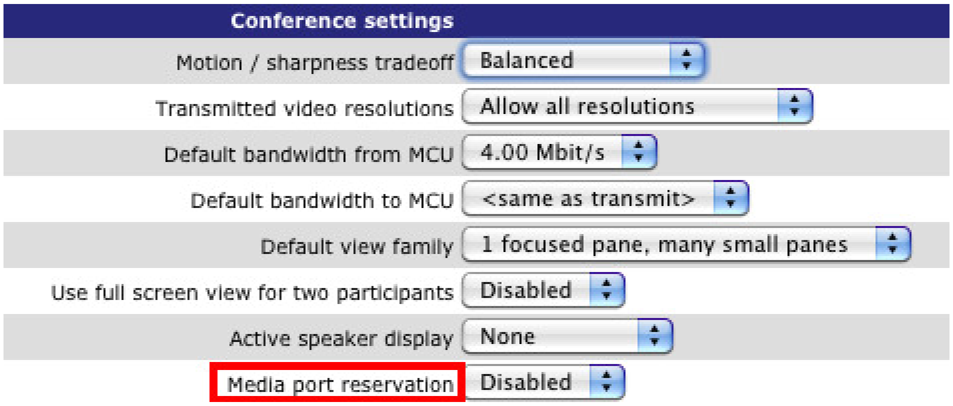
1. Go to **Settings > H.323**.
2. Set **H.323 gatekeeper usage** to *Disabled*.



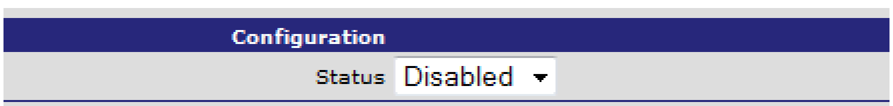
3. Click **Apply changes**.

Task 5: 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**.

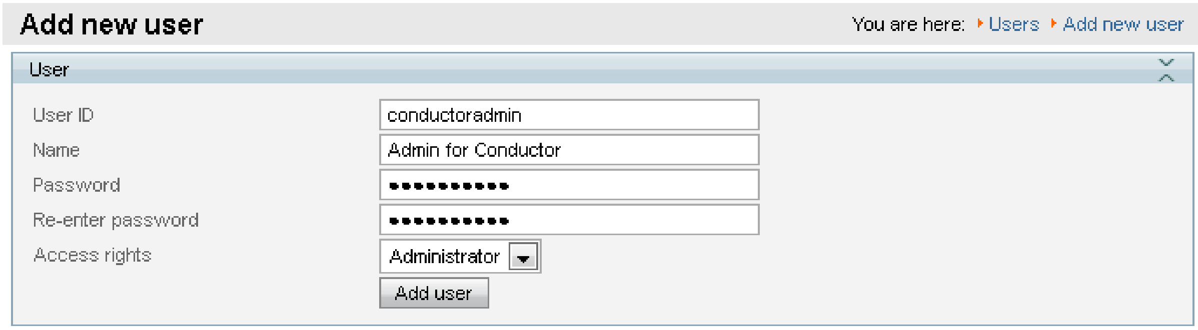
Configuring the TelePresence Server

Task 6: 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*.



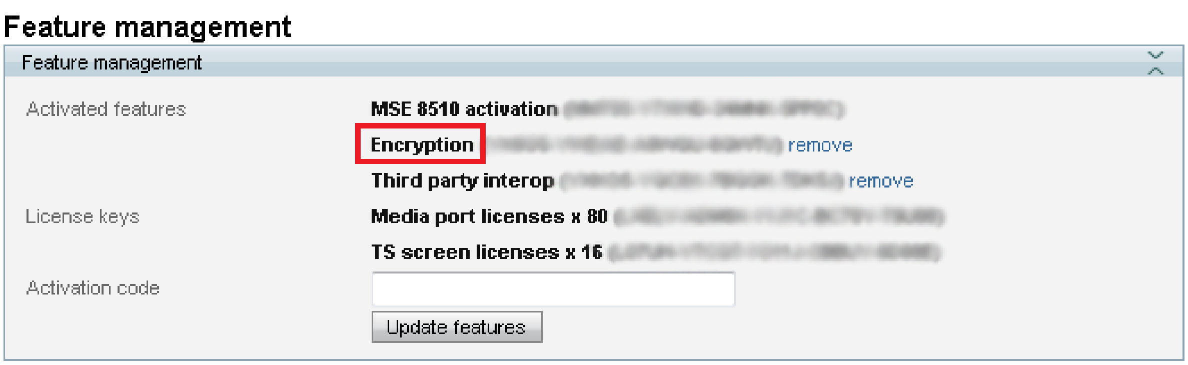
4. Click **Add user**.
5. Repeat the steps for any other TelePresence Servers.

Task 7: 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. 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, perform the following tasks:

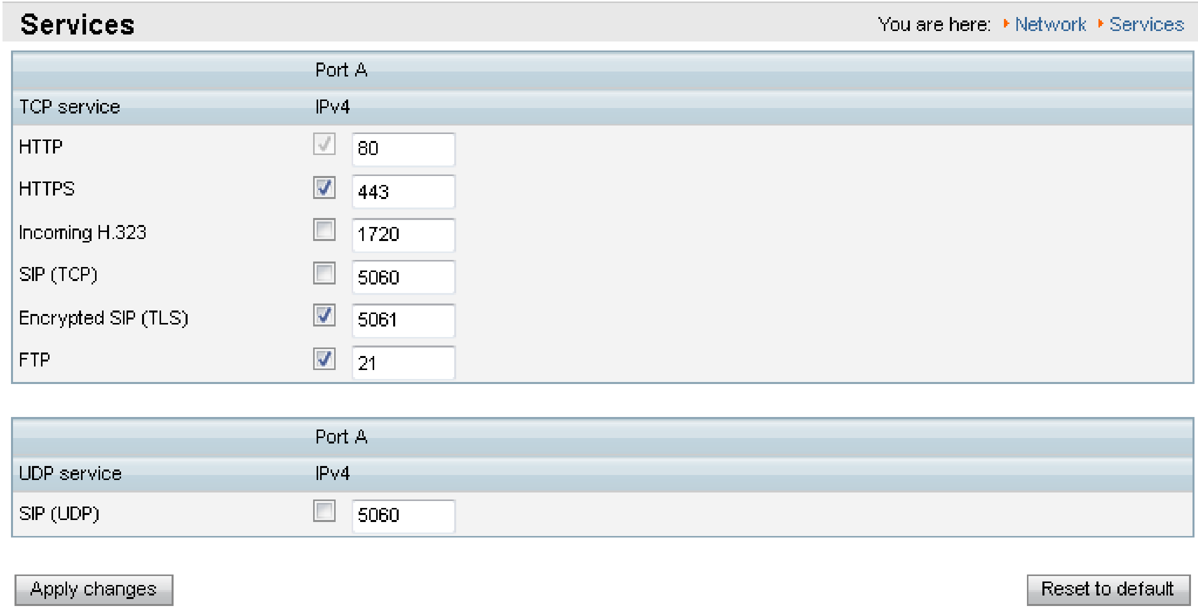
1. Go to **Configuration > Upgrade**.
2. Go to the **Feature management** section and verify that the **Encryption** key is installed. If the key is not installed, enter the **Activation code** and click **Update features**.



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.

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



5. Click **Apply changes**.

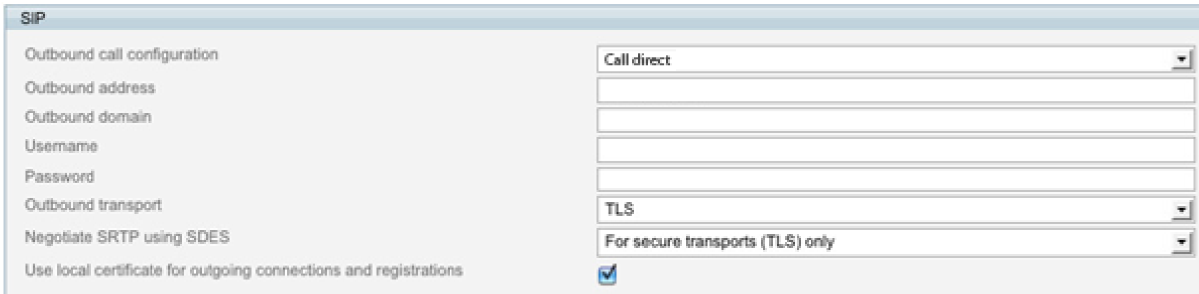
Task 8: Configuring SIP

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.
Outbound address	Leave blank.
Outbound domain	Leave blank.
Username	Leave blank.
Password	Leave blank.
Outbound transport	Select *TLS* from the drop-down list.
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.



3. Click **Apply changes**.

Task 9: Disabling H.323 registration

Perform the following steps to enable 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**.
5. Repeat the steps for any other TelePresence Servers.

Task 10: Configuring the operational mode

(This task is not relevant for Cisco TelePresence Server on Virtual Machine or Cisco TelePresence Server on Multiparty Media 310/320.)

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.
9. Repeat the steps for any other TelePresence Servers.

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 Getting Started Guide*.

Task 11: 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 12: 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.

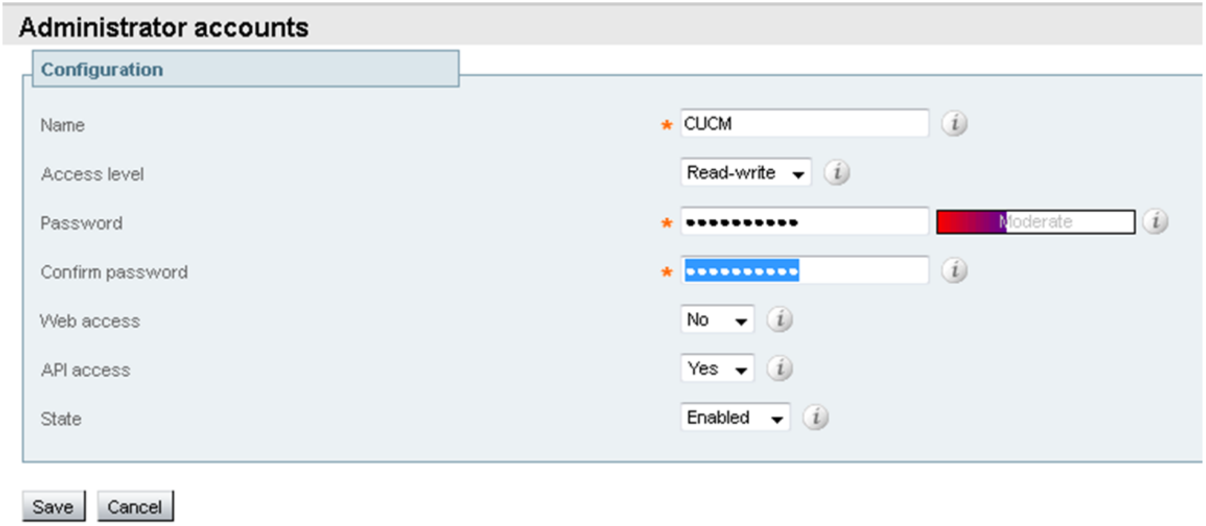
Note: the TelePresence Conductor will not handle conference requests if it has the root password set to its default value.

Task 13: 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.
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*.

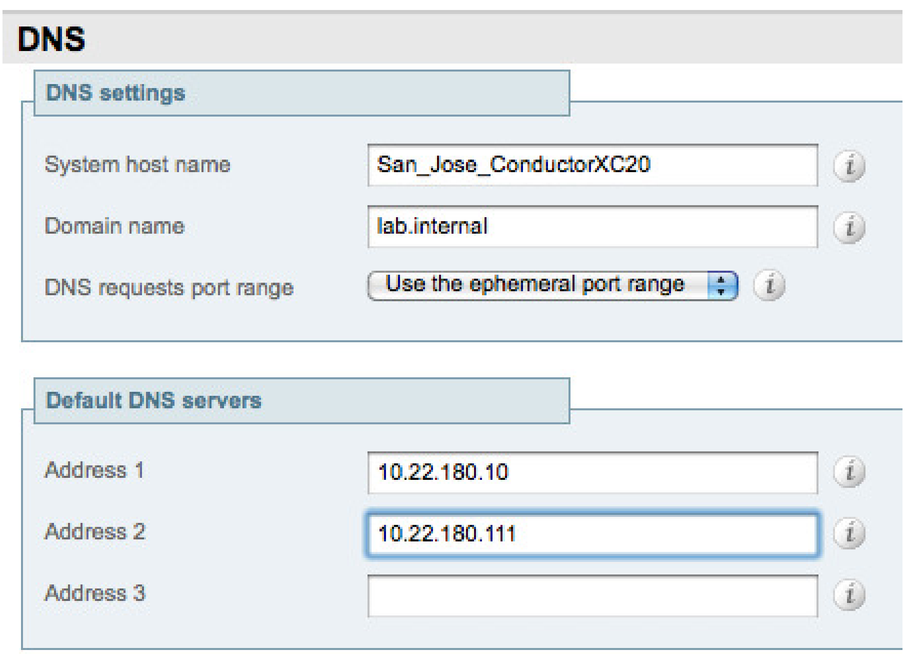


5. Click **Save**.

Task 14: 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.

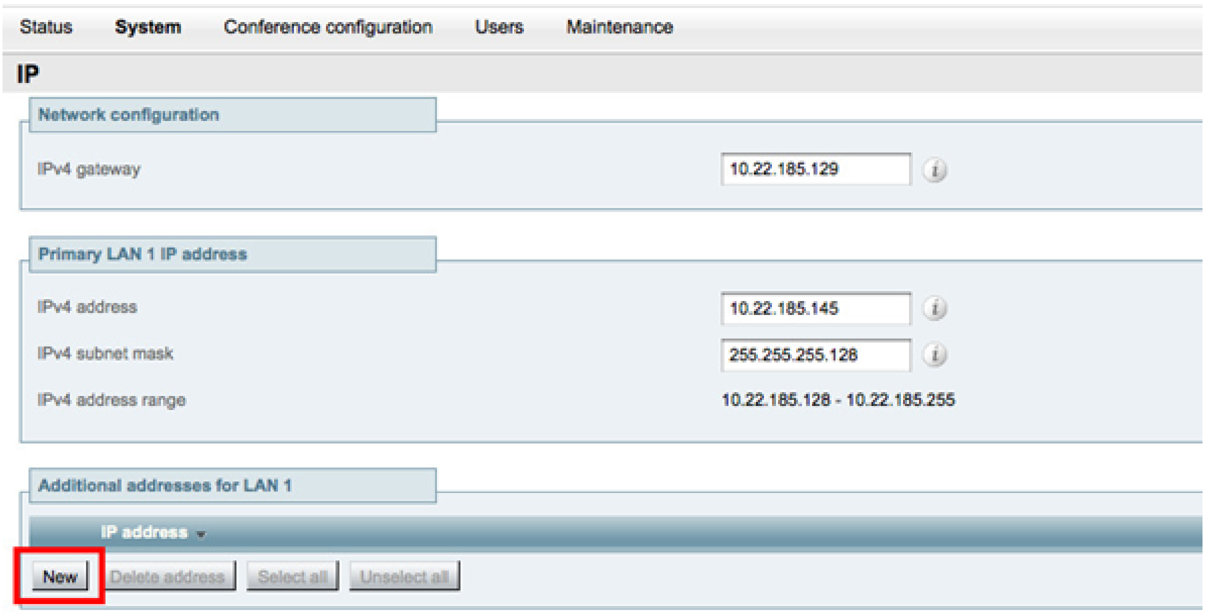


Note: the FQDN of the TelePresence Conductor will be <System host name>.<Domain name>

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

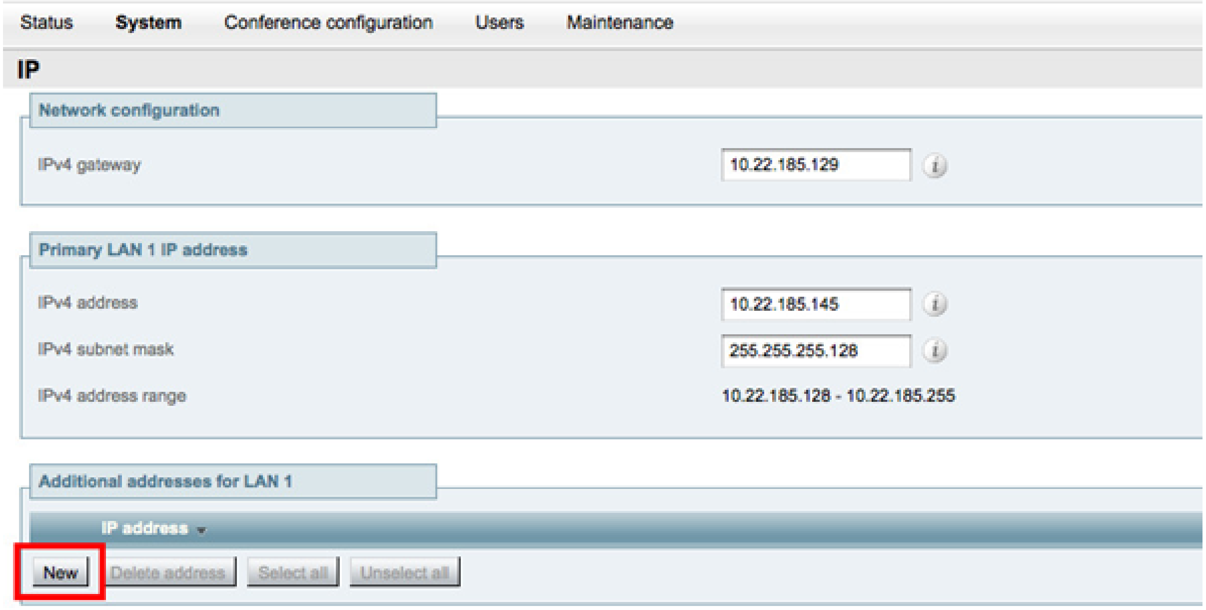
1. Go to **System > IP**.
2. In the **Additional addresses for LAN 1** section click **New**.



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**.

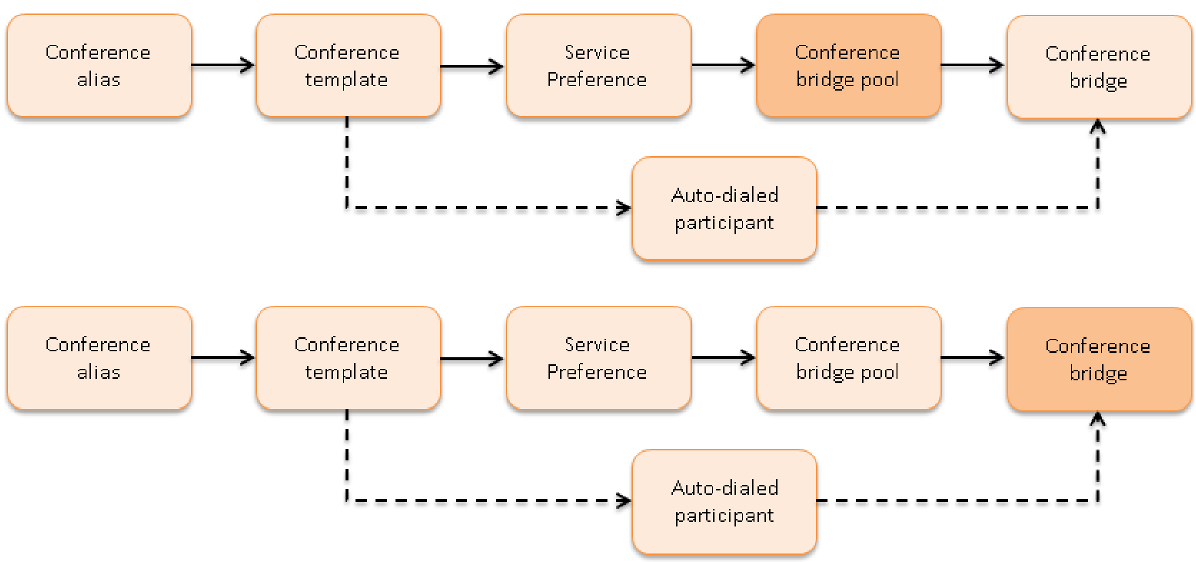
5. Repeat steps 2 through 4 until you have added IP addresses for ad hoc and rendezvous handling for each Location to be supported.

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 16: Setting up conference bridge pools



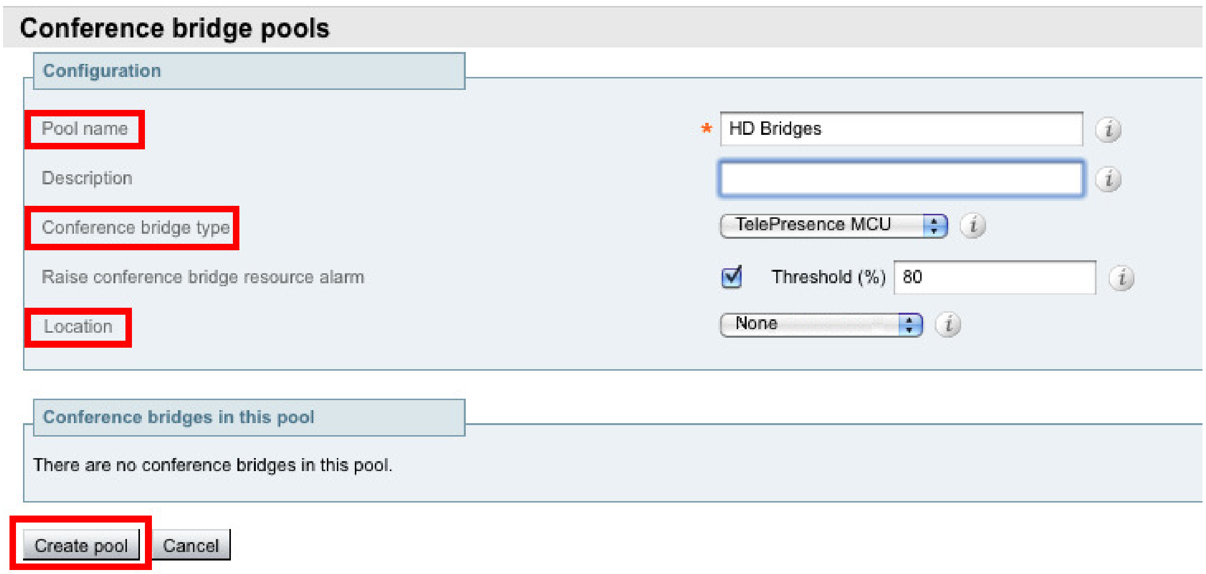
To set up a conference bridge pool, you need to create a conference bridge pool and then add one or more conference bridge(s) to it. The following examples show how to set up conference bridge pools for:

- TelePresence MCU hosted conferences
- TelePresence Server hosted conferences

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.



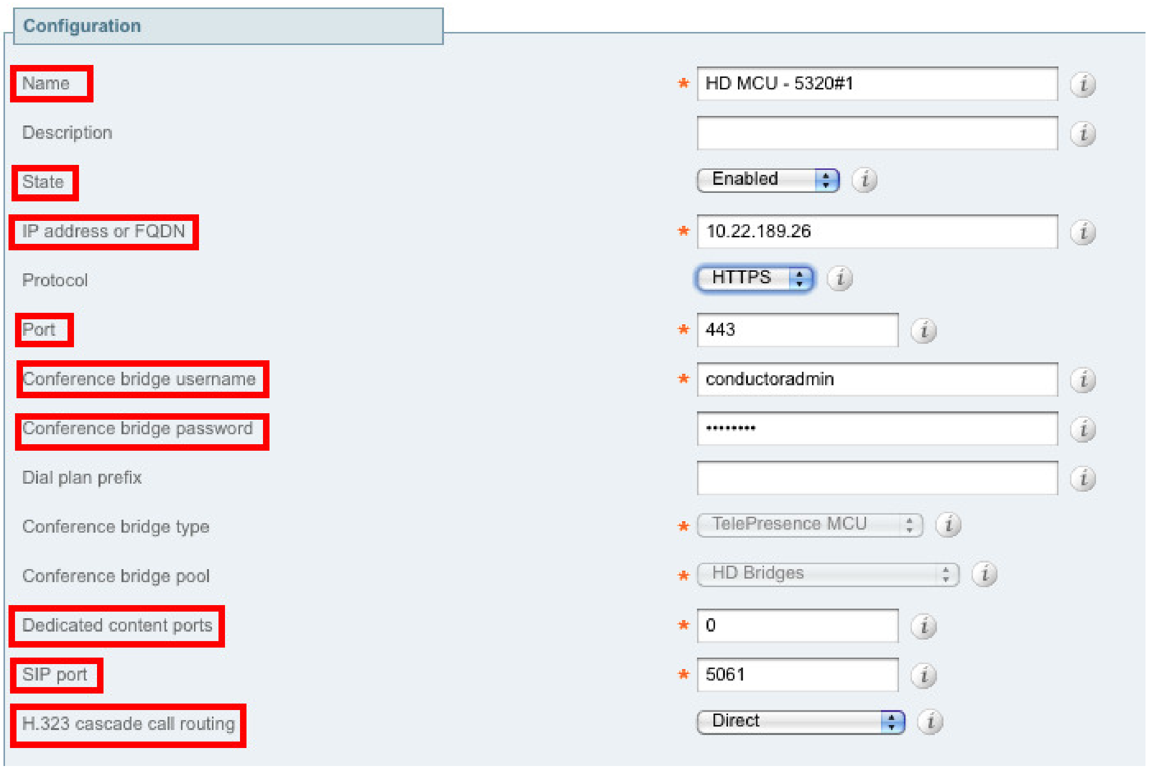
4. Click **Create pool**.

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 1: Creating a user [p.11]).

Conference bridge Password	Enter the conference bridge password for this user.
Dedicated content ports	Enter the appropriate value for your TelePresence MCU.
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 TelePresence MCU to TelePresence MCU 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.

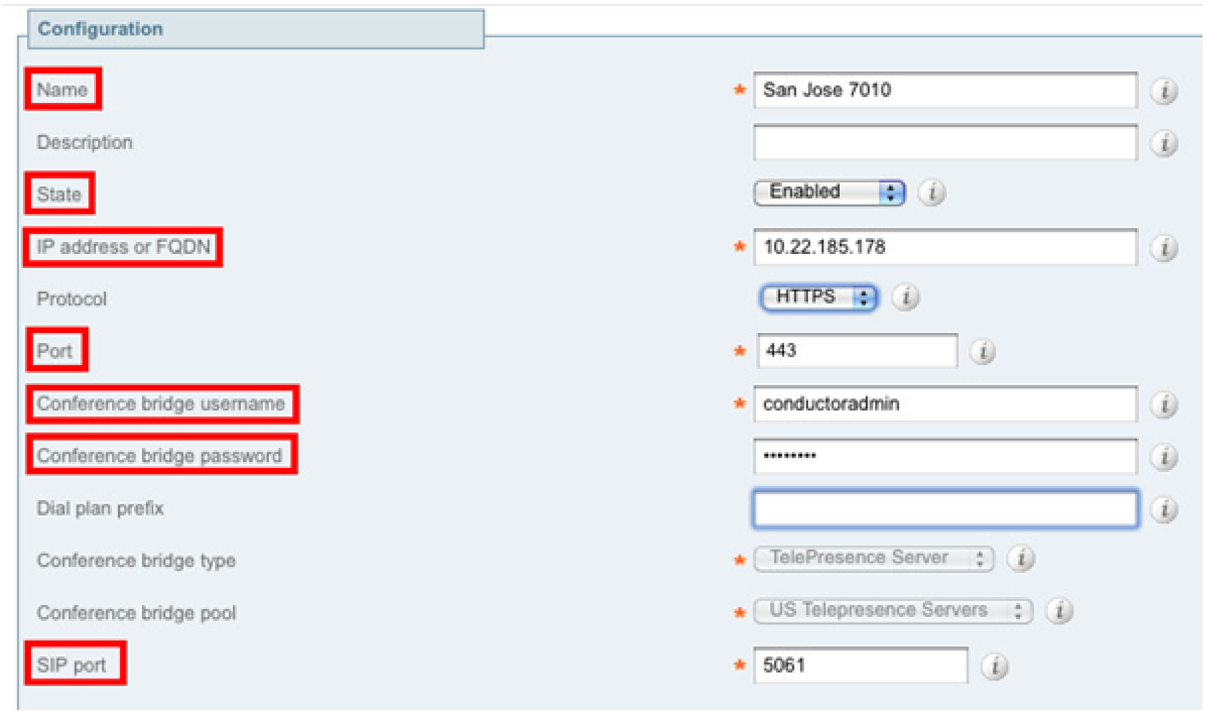
4. Click **Create pool**.

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 10: Configuring the operational mode [p.17]).

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 6: Creating a user [p.14]).
Conference bridge Password	Enter the conference bridge password for this user.
Dedicated content ports	Enter the appropriate value for your TelePresence Server.
SIP Port	Enter the SIP port on which the TelePresence Server is to listen for SIP TLS traffic, typically this is '5061'.



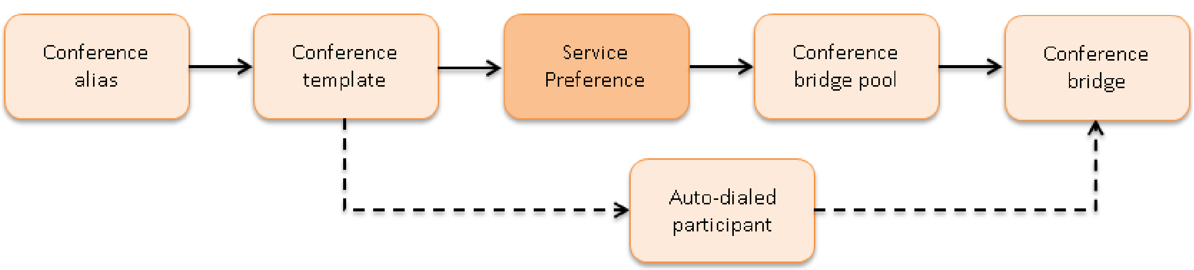
3. Click **Create conference bridge**.
4. Ensure that under the **Conference bridges in this pool** section, under the **Status** header the conference bridge is listed as *Active*.

Conference bridges in this pool

Name	Address	State	Username	Dial plan prefix	Status	Status detail	Last unsuccessful contact attempt
San Jose 7010	10.22.185.178	Enabled	conductoradmin		Active		2012-10-02 15:32:28

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. For TelePresence MCUs a conference can be cascaded from one TelePresence MCU to another, taking into account the prioritized list of conference bridge pools. Cascading between TelePresence Servers is not supported, because TelePresence Server versions 3.0 and 3.1 do not have this feature.

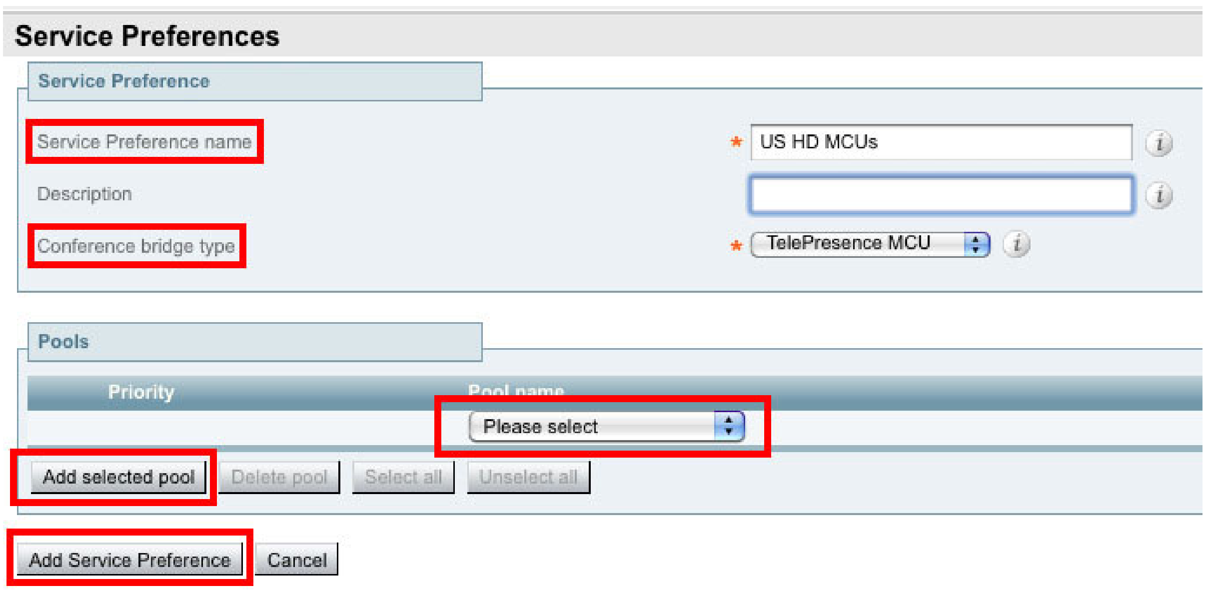
The following examples show how to create Service Presences for:

- 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 the appropriate bridge type, *TelePresence MCU*.
Pool name	Select the appropriate pool from the drop-down list.

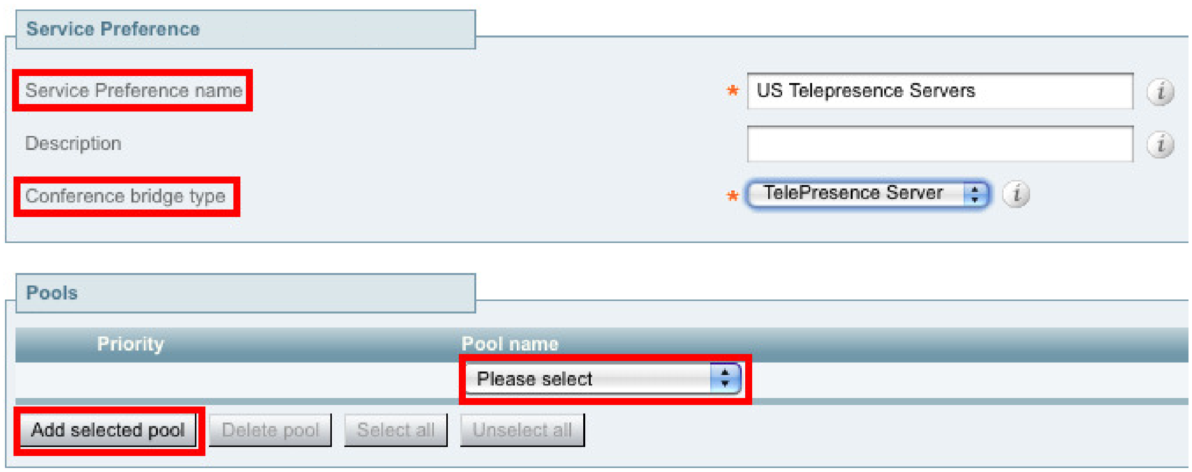


4. Click **Add selected pool**.
5. Click **Save**.

Adding a TelePresence Server Service Preference

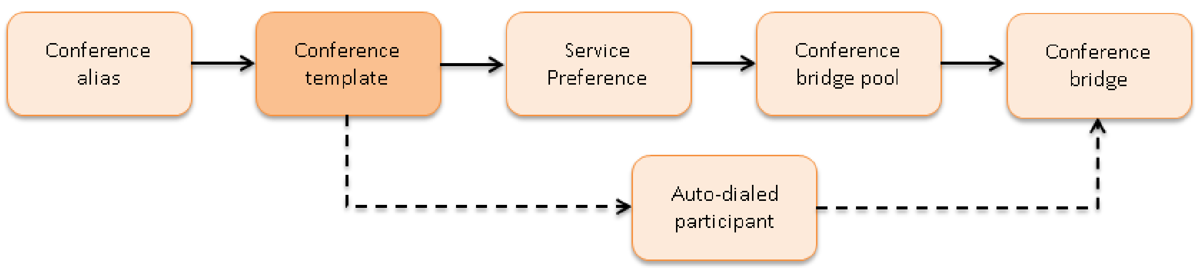
1. Go to **Conference configuration > Service Preferences**.
2. Click **New**.
3. Enter the following values into the relevant fields:

Service Preference name	Enter the name of the Service Preference.
Conference bridge type	Select the appropriate bridge type, *TelePresence Server*.
Pool name	Select the appropriate pool from the drop-down list.



4. Click **Add selected pool**.
5. Click **Save**.

Task 18: Creating conference templates



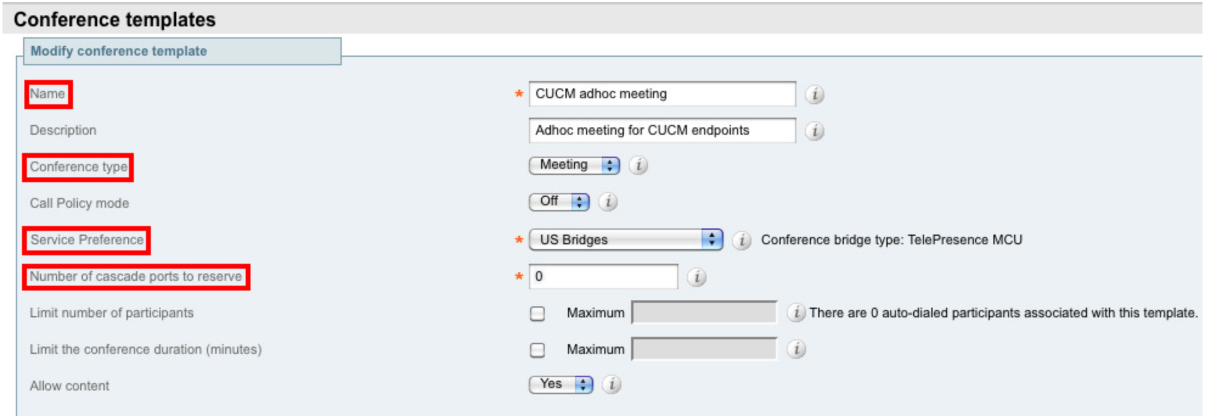
The following examples show how to create conference templates for:

- ad hoc Meeting-type conferences
- rendezvous Meeting-type conferences

Creating a 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 type (it can be a TelePresence Server or a TelePresence MCU pool).
Number of cascade ports to reserve	(Only available if the Service Preference selected is for TelePresence MCU(s)) Enter '0' to disable cascade port reservation. This is required because cascading is not supported for ad hoc conferences.

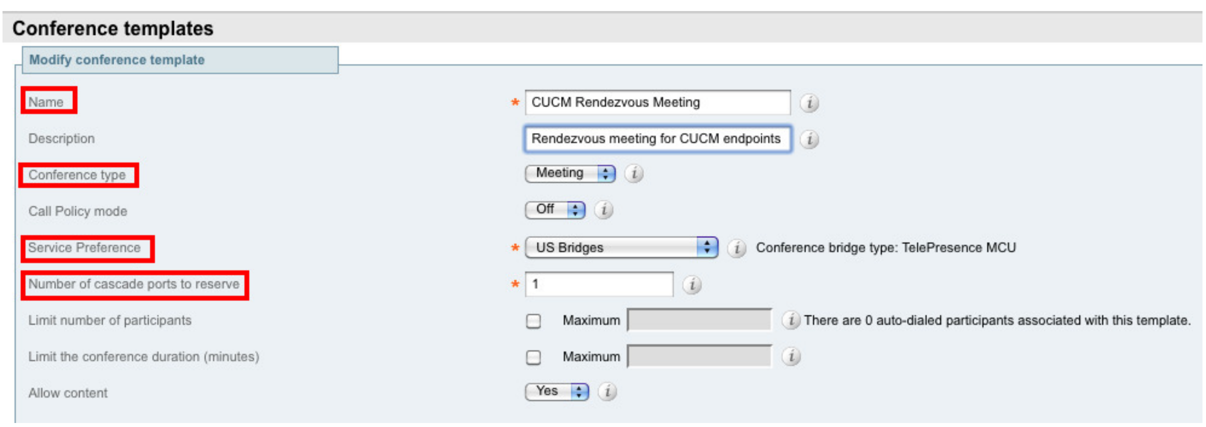


4. Configure other entries as required.
5. Click **Create conference template**.

Creating a conference template for a rendezvous Meeting-type conference

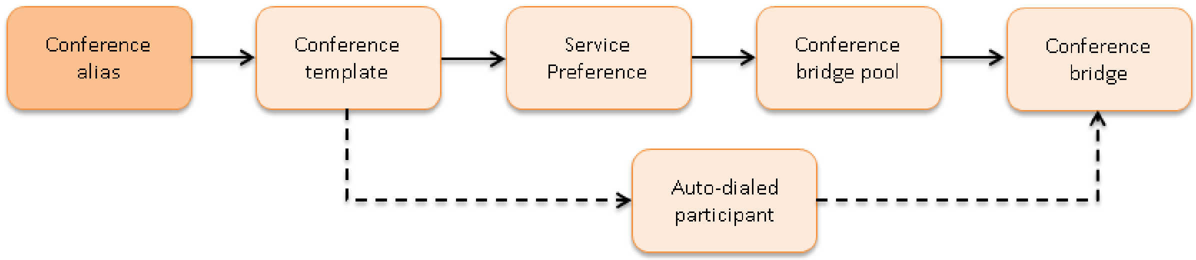
1. Go to **Conference configuration > Conference templates**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

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 Chairperson alias).
Service Preference	Select the appropriate Service Preference for this template type (it can be a TelePresence Server or a TelePresence MCU pool).
Number of cascade ports to reserve	(Only available if the Service Preference selected is for TelePresence MCU(s)) To enable cascade port reservation, enter 1 (the default), or a higher number if you want to cascade to more than one TelePresence MCU. To disable cascade port reservation, enter '0'.



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

Task 19: Creating conference aliases

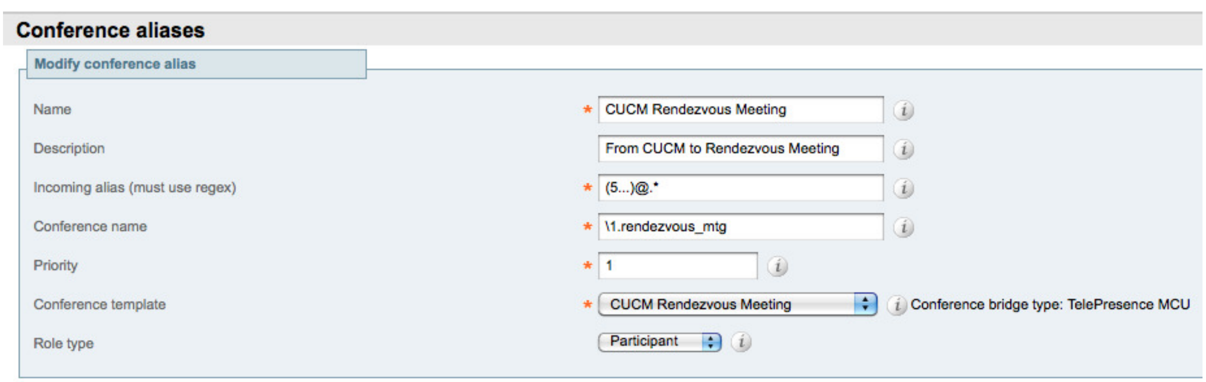


The following example shows how to create a conference alias for a rendezvous Meeting-type conference.

Creating a conference alias for a rendezvous Meeting-type conference

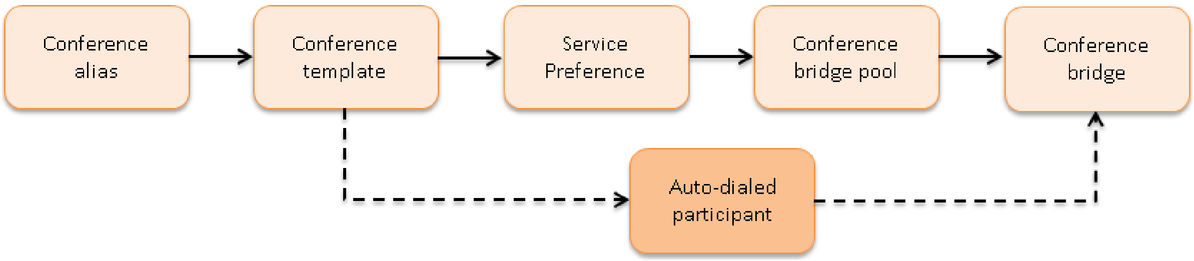
1. Go to **Conference configuration > Conference aliases**.
2. Click **New**.
3. Enter the following into the relevant fields, leave other fields as their default values:

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 20: Creating auto-dialed participants

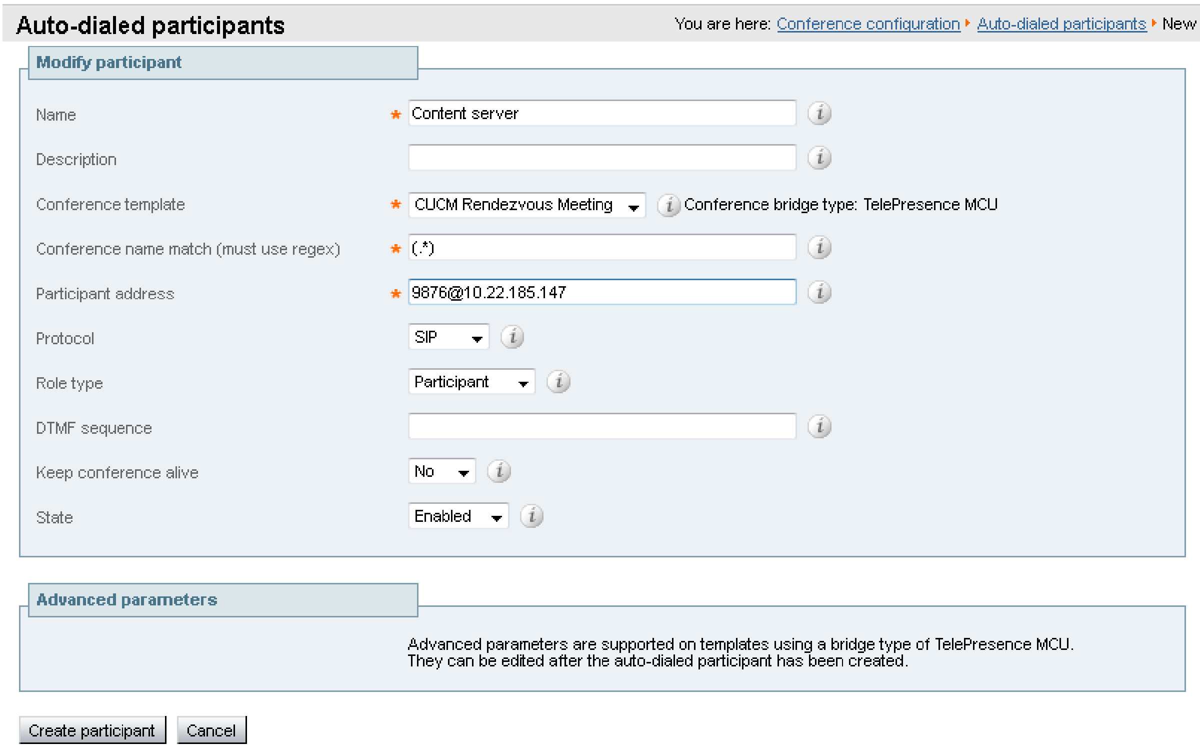


The following example shows how to create an auto-dialed participant for a rendezvous Meeting-type conference.

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*.



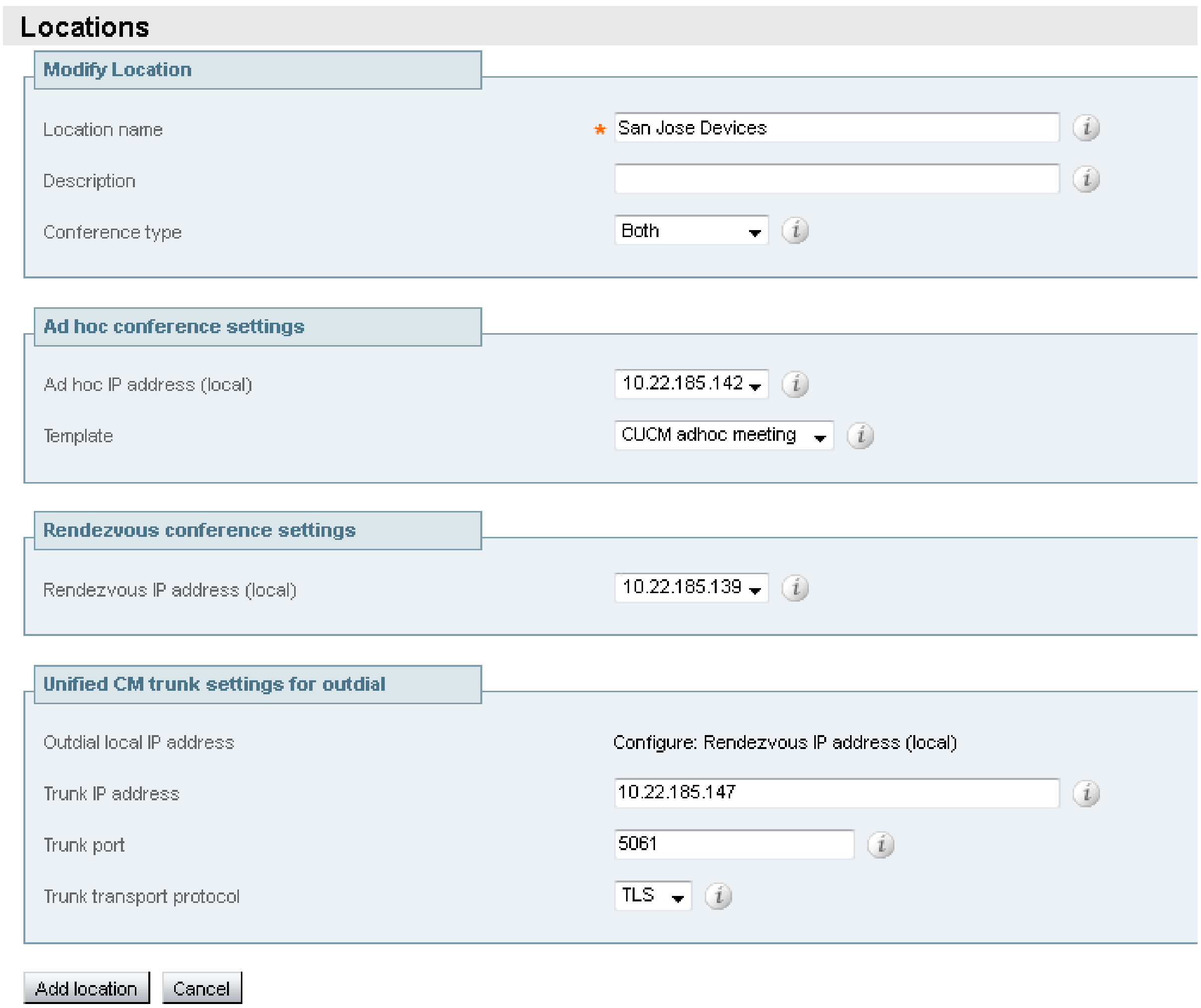
4. Click **Create participant**.

Task 21: Creating Locations in TelePresence Conductor

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*, *Rendezvous*, or *Both*, from the drop-down list. In this example *Both* was selected. **Note:** *Both* must be selected for ad hoc conferences with outbound calls.
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.
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 IP address	Only needed for calls out-dialed from TelePresence Conductor / conference bridge to Unified CM. Enter the IP address of Unified CM. **Note:** this address is the address of Unified CM and is used by TelePresence Conductor to forward calls to Unified CM for auto-dial participants and any other out-dialed calls such as those initiated by Cisco TMS.
Trunk port	Enter the receiving signaling port of 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 22: 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.

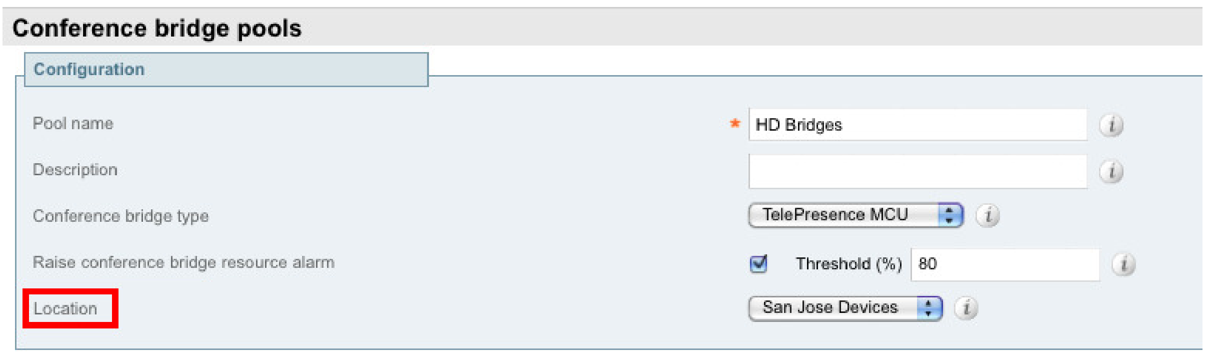
Examples of outbound calls are:

- 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 Task 21: Creating Locations in TelePresence Conductor [p.31]) 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

Task 23: Adding the Unified CM normalization script

Follow the instructions in Appendix 2: Adding the Unified CM normalization script [p.63] to add the Unified CM normalization script to Unified CM.

Task 24: 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.

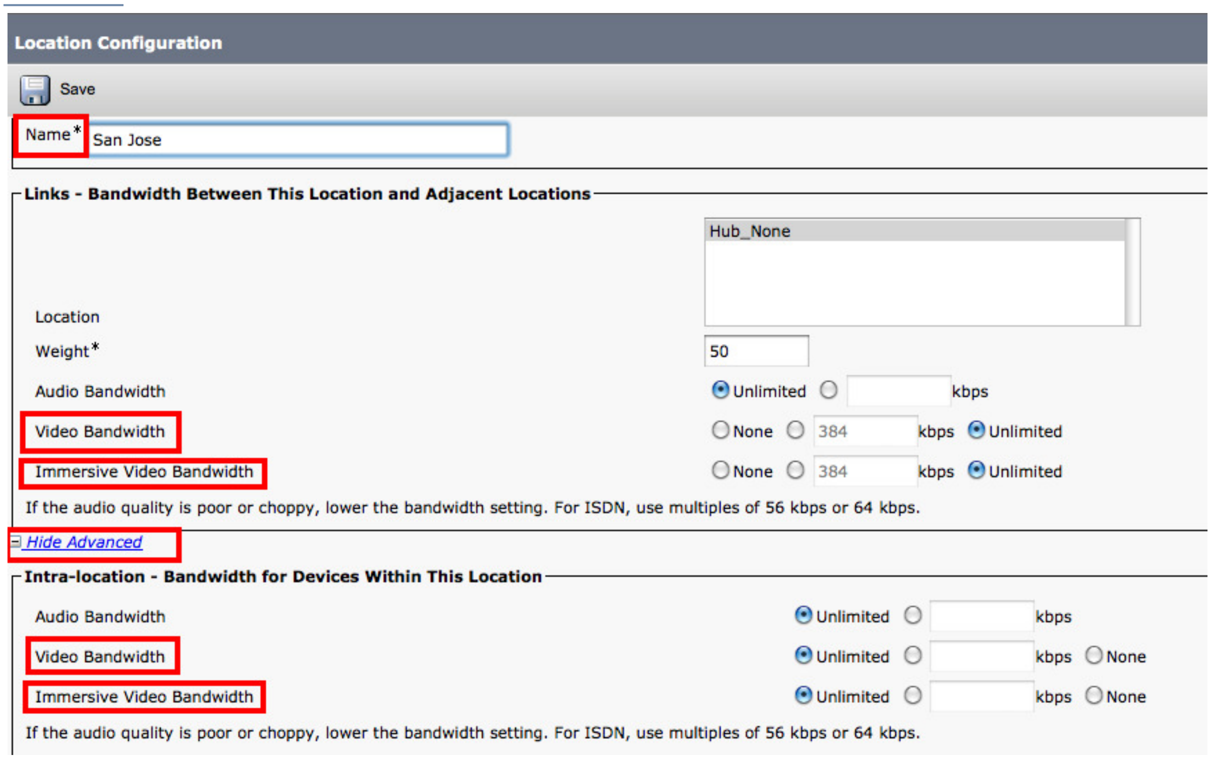
To view a location in Unified CM:

1. Go to the Unified CM web interface and log in as an admin user.
2. Go to **System > Location Info > Location**.
3. 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 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 25: Ensuring that Unified CM trusts the TelePresence Conductor server certificate

For Unified CM to make a TLS connection to TelePresence Conductor, Unified CM must trust the TelePresence Conductor's server certificate. Unified CM must therefore trust a root certificate that in turn trusts the TelePresence Conductor's certificate. See *Cisco TelePresence Conductor Certificate Creation and Use Deployment Guide* for details of generating CSRs on TelePresence Conductor to acquire certificates from a Certificate Authority (CA), as well as information about operating private Certificate Authorities.

TelePresence Conductor and Unified CM must both have valid server certificates loaded and the root CA of the TelePresence Conductor server certificate must be loaded onto Unified CM.

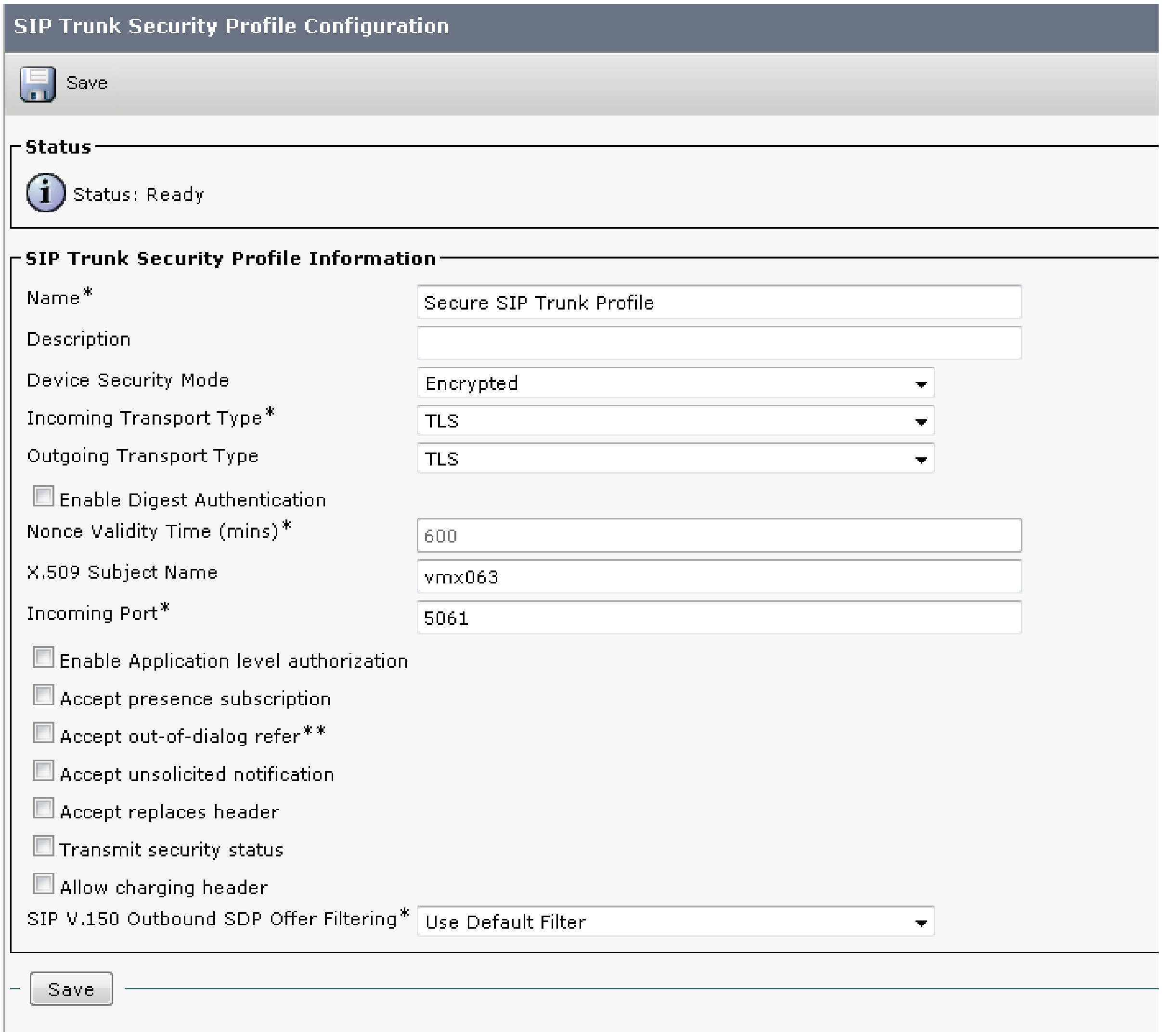
Note that in a clustered environment, you must install CA and server certificates on each peer/node individually.

Task 26: 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 Unified CM 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 27: Adding the TelePresence Conductor as a Conference bridge to Unified CM for ad hoc conferences

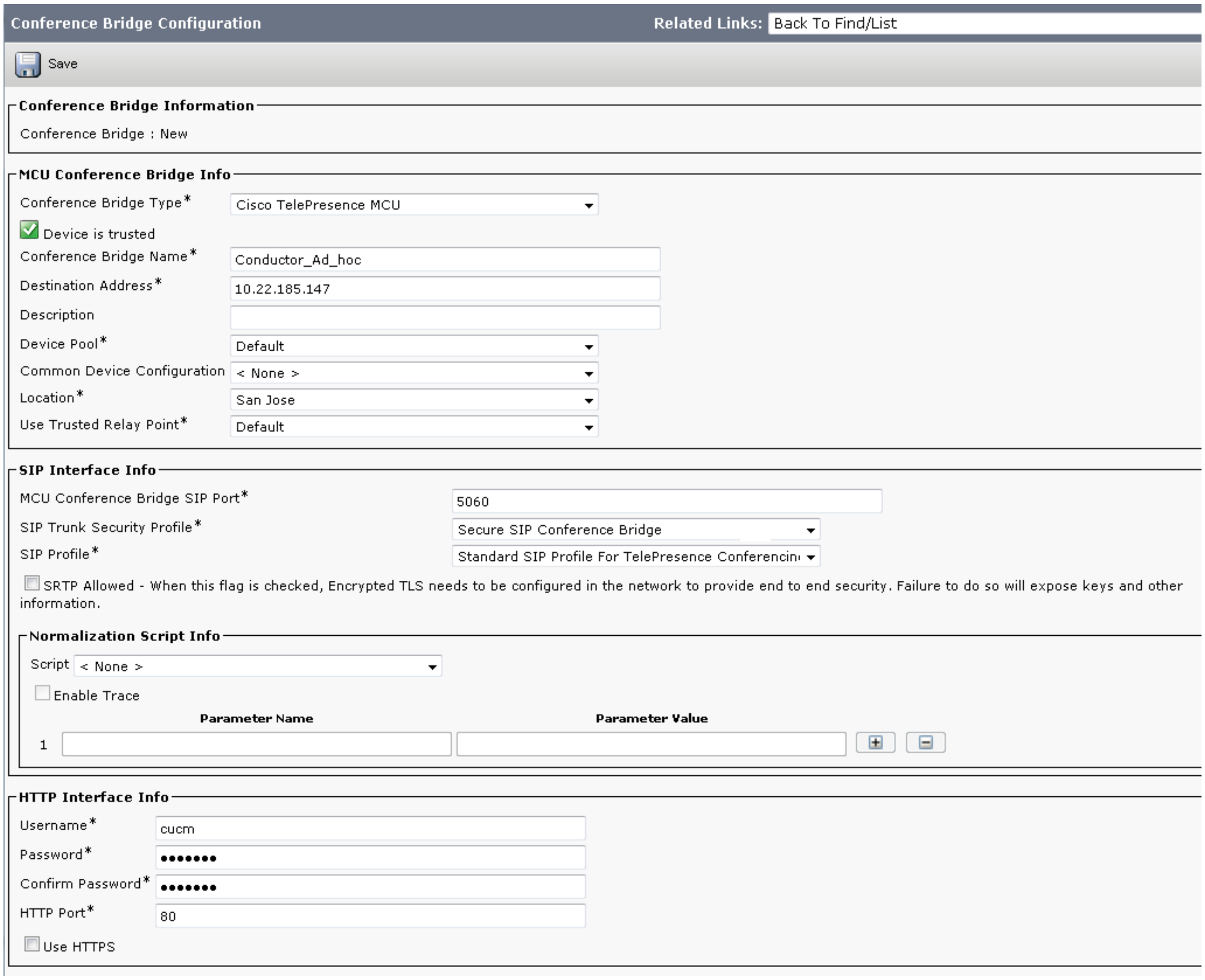
Note: The instructions in this step are for Unified CM version 9.0. For Unified CM version 8.6.2, go to Appendix 1: Unified CM version 8.6.2 configuration [p.61]

For Unified CM version 9.0:

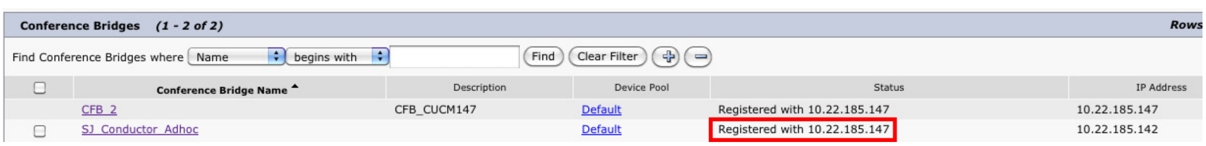
1. Go to **Media Resources > Conference Bridge**.
2. Click **Add New** to create a new conference bridge.
3. Enter the following into the relevant fields, leave other fields as their default values:

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’.



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

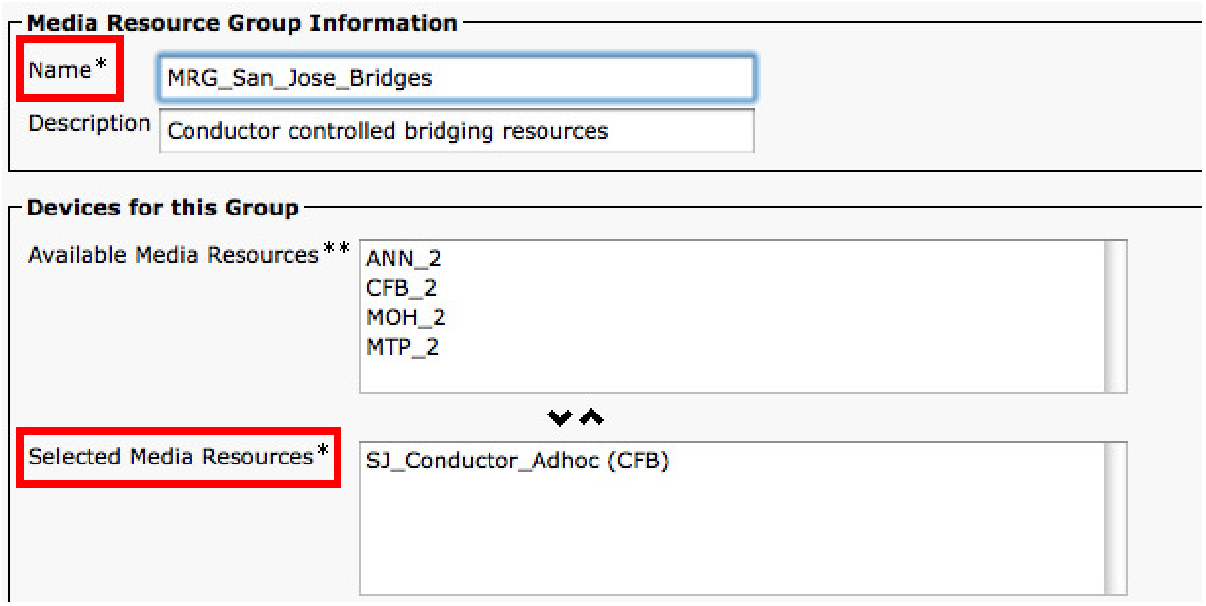


Task 28: Adding the TelePresence Conductor to an MRG and MRGL

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.

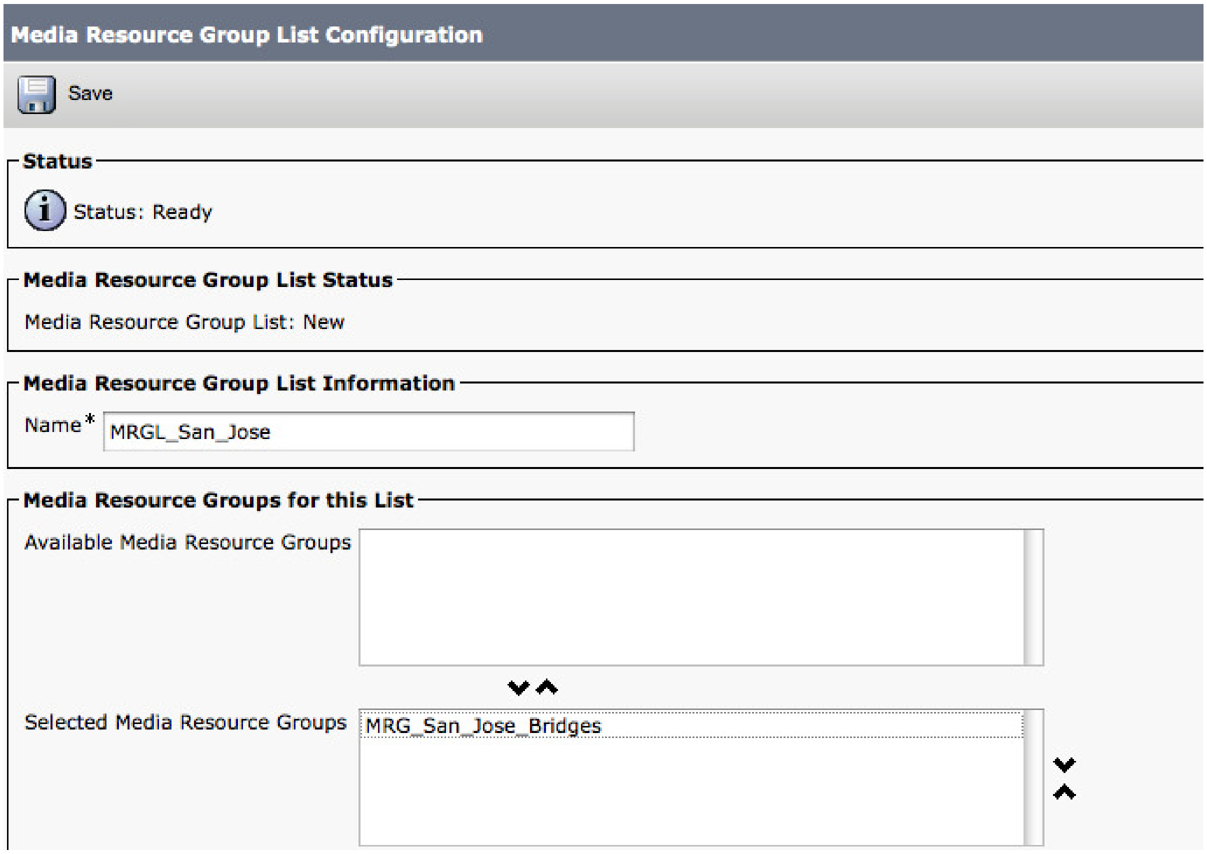
4. Move the TelePresence Conductor media bridge (the conference bridge configured in Task 27: Adding the TelePresence Conductor as a Conference bridge to Unified CM for ad hoc conferences [p.36]) down to the **Selected Media Resources** box.



5. Click **Save**.

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

6. Go to **Media Resources > Media Resource Group Lists**.
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**.

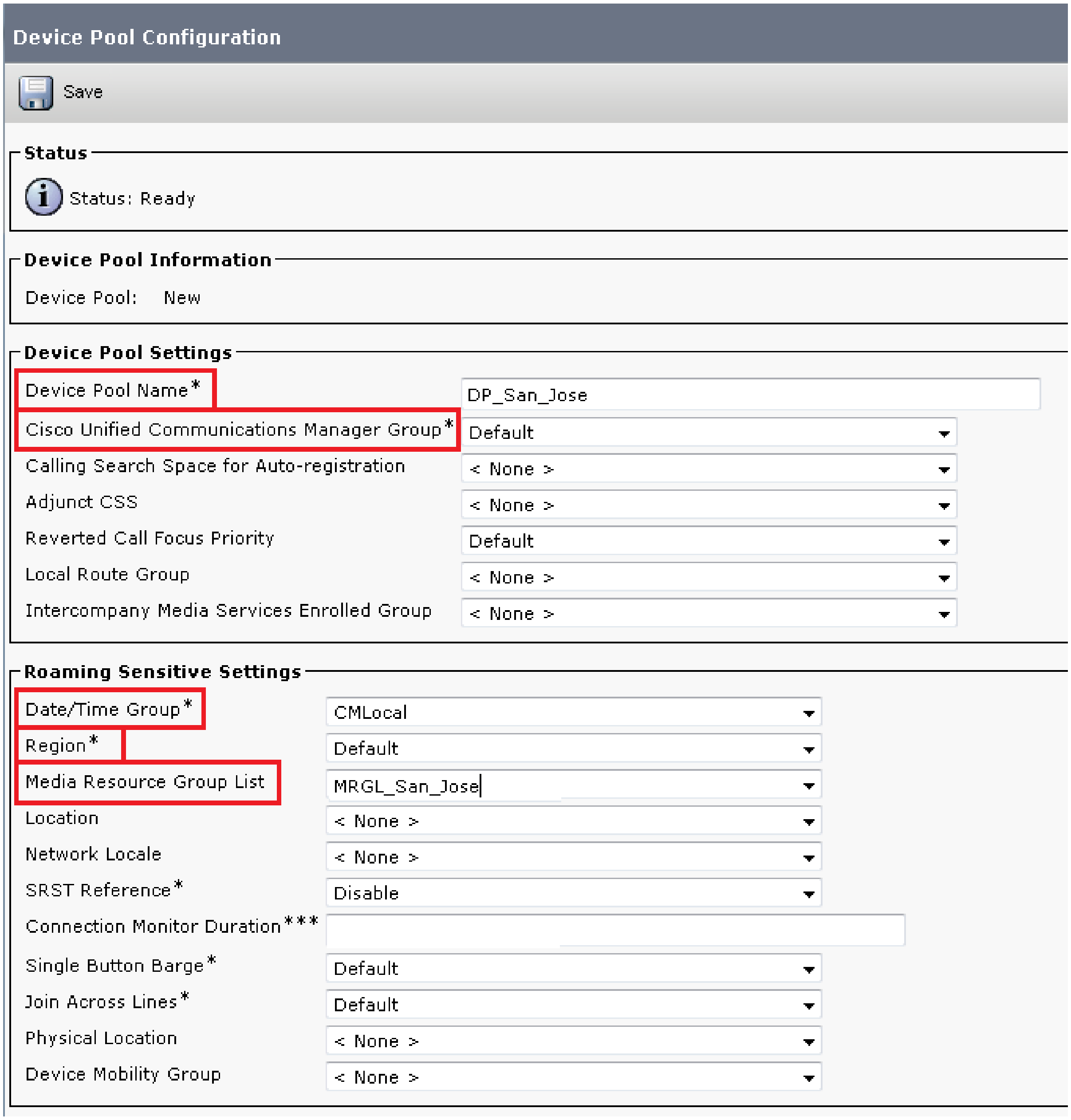
Task 29: Adding an MRGL to a Device Pool or Device

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 under.

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 Name	Enter a Device pool name.
Cisco Unified Communications Manager Group	Select the appropriate group from the drop-down list.
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 28: Adding the TelePresence Conductor to an MRG and MRGL [p.38] (steps 6 -10) from the drop-down list.



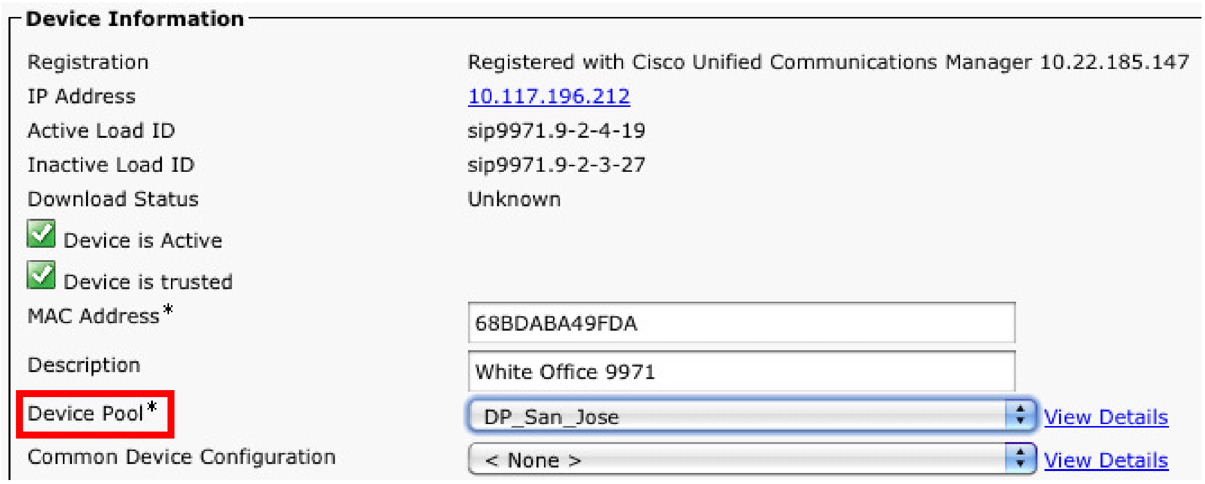
4. Click **Save** and **Reset** for the changes to take effect.

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.

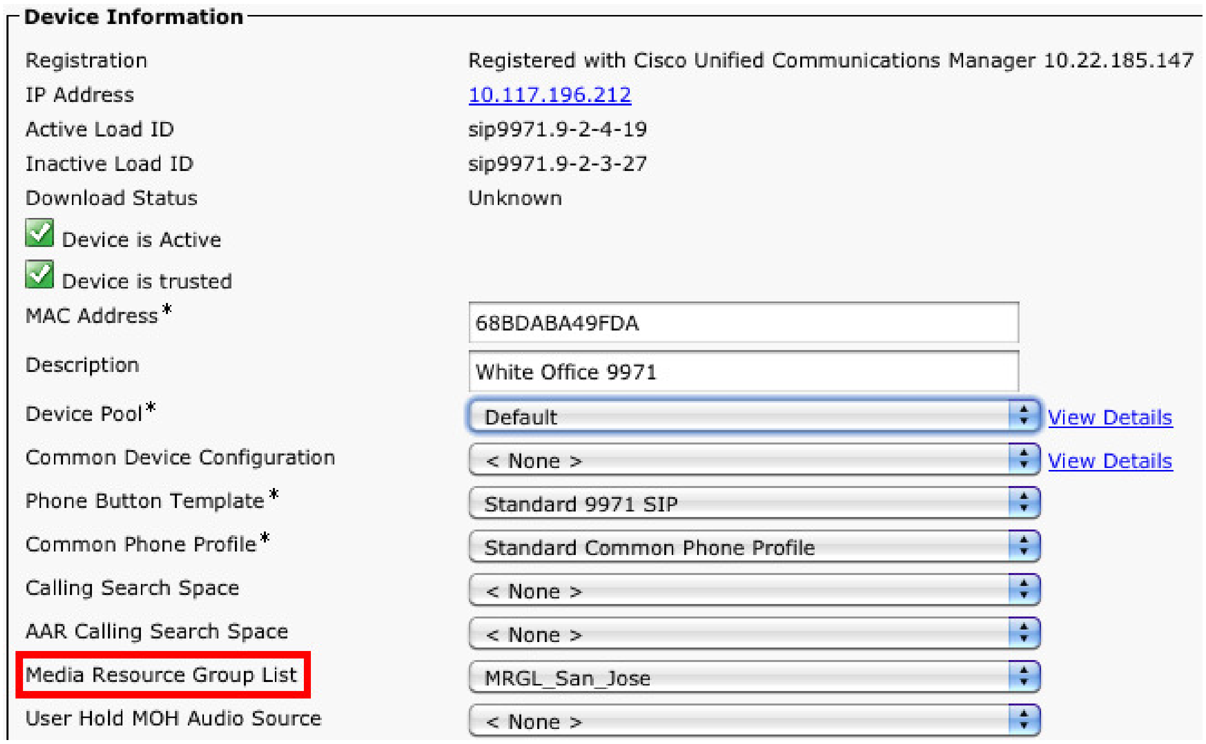


8. Click Save.
9. Click **Apply Config**.
10. Click **Reset** for the changes to take effect.
    Note: This will reboot the phones when applied.

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.

11. Go to **Device > Phones**.
12. Click **Find** and select the device to change the MRGL settings on.
13. Select the MRGL used in Task 28: Adding the TelePresence Conductor to an MRG and MRGL [p.38] (steps 6 – 10) from the drop-down list.



14. Click **Save**.
15. Click **Apply Config**.
16. Click **Reset** for the changes to take effect.

Task 30: Creating a new SIP profile

The TelePresence Conductor will wait for 30 seconds for a call to appear on the conference bridge, otherwise it will assume that the call is not going to arrive. You must create a new SIP profile with a 30 second timeout so that you can then apply this to the SIP trunk from Unified CM to TelePresence Conductor. To do this:

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**.

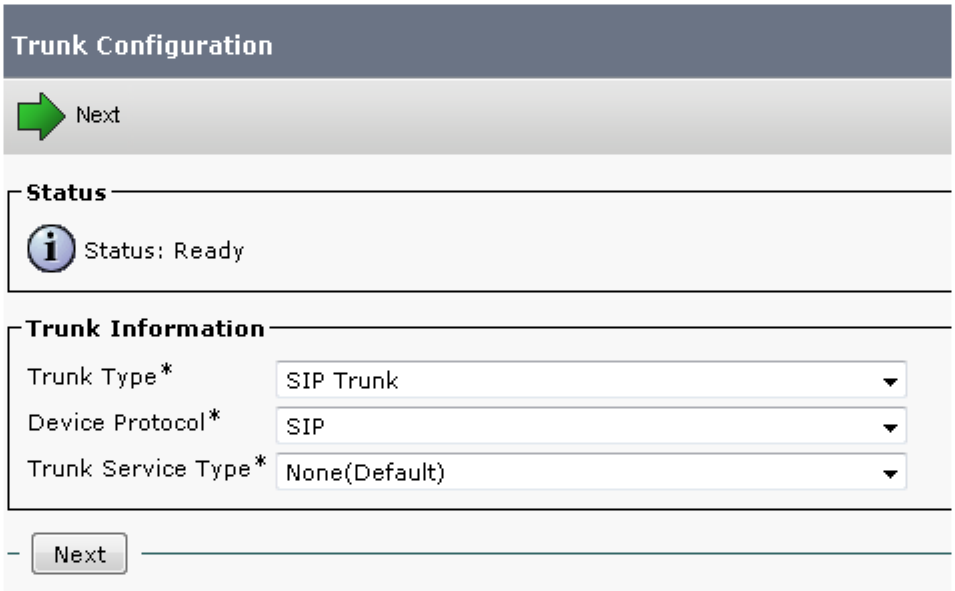
Task 31: Adding a SIP trunk to TelePresence Conductor for rendezvous conferences (and to receive TelePresence Conductor out-dialed calls)

To configure a SIP trunk to the TelePresence Conductor:

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

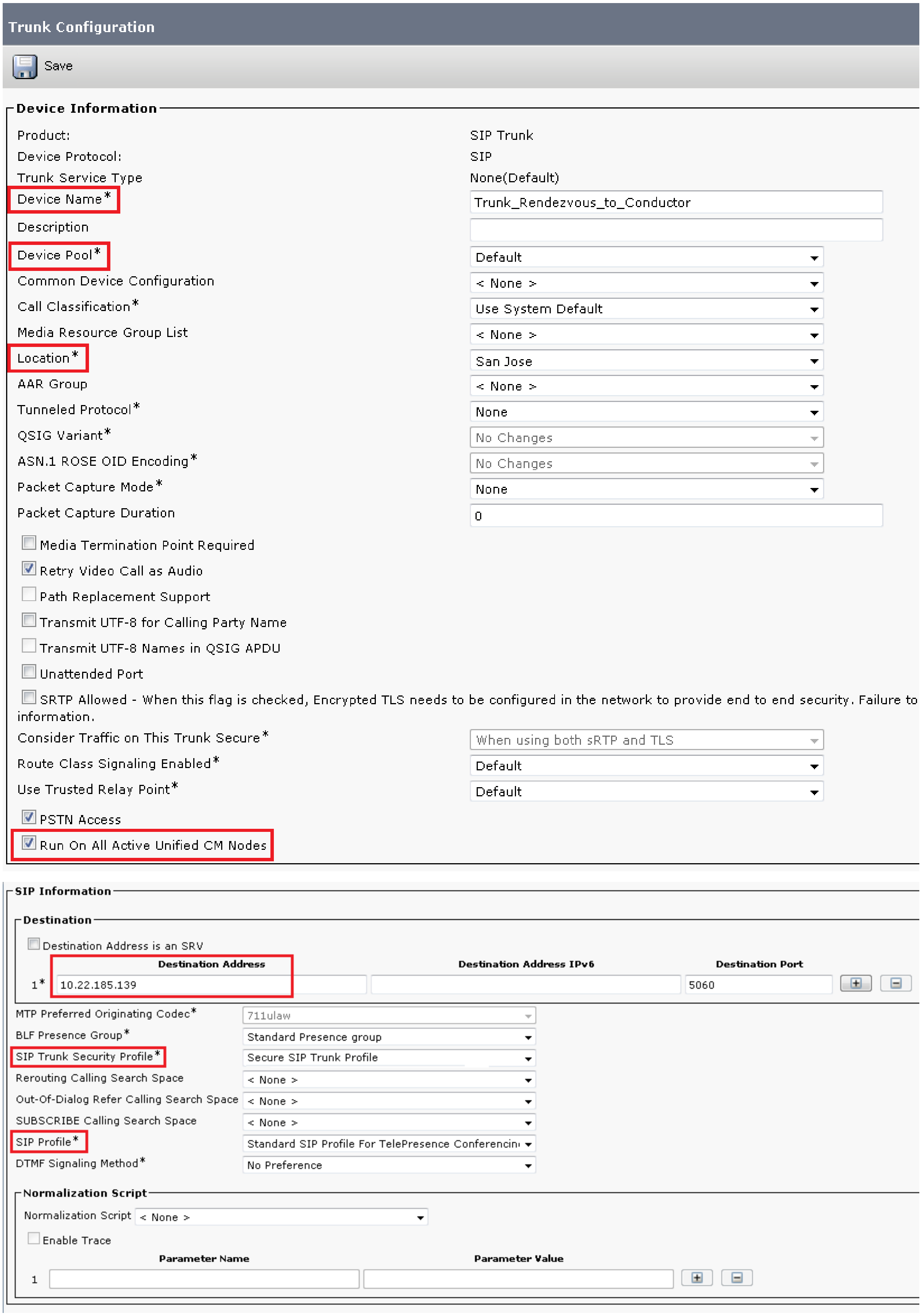
3. Enter the following into the relevant fields:

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 Name	Enter a trunk name.
Device Pool	Select the appropriate Device Pool.
Location	Select the Location found in Task 24: Viewing a location in Unified CM [p.33].
Run On All Active Unified CM Nodes	Check this setting.
Destination Address	Enter the TelePresence Conductor's location-specific rendezvous IP address. This IP address is the one configured on the TelePresence Conductor's **Locations** page (**Conference configuration > Locations**) in the **Rendezvous conference settings** section. (See Task 21: Creating Locations in TelePresence Conductor [p.31])
SIP Trunk Security Profile	Select the *Secure SIP Trunk Profile* from the drop-down list.
SIP Profile	Select the SIP Profile created in Task 30: Creating a new SIP profile [p.43].


Trunk Configuration
Save
Device Information
Product:
SIP Trunk
Device Protocol:
SIP
Trunk Service Type
None(Default)
Device Name*
Trunk_Rendezvous_to_Conductor
Description
Device Pool*
Default
Common Device Configuration
< None >
Call Classification*
Use System Default
Media Resource Group List
< None >
Location*
San Jose
AAR Group
< None >
Tunneled Protocol*
None
QSIG Variant*
No Changes
ASN.1 ROSE OID Encoding*
No Changes
Packet Capture Mode*
None
Packet Capture Duration
0
Media Termination Point Required
Retry Video Call as Audio
Path Replacement Support
Transmit UTF-8 for Calling Party Name
Transmit UTF-8 Names in QSIG APDU
Unattended Port
SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to
information.
Consider Traffic on This Trunk Secure*
When using both sRTP and TLS
Route Class Signaling Enabled*
Default
Use Trusted Relay Point*
Default
PSTN Access
Run On All Active Unified CM Nodes
SIP Information
Destination
Destination Address is an SRV
Destination Address
Destination Address IPv6
Destination Port
1*
10.22.185.139
5060
MTP Preferred Originating Codec*
711ulaw
BLF Presence Group*
Standard Presence group
SIP Trunk Security Profile*
Secure SIP Trunk Profile
Rerouting Calling Search Space
< None >
Out-Of-Dialog Refer Calling Search Space
< None >
SUBSCRIBE Calling Search Space
< None >
SIP Profile*
Standard SIP Profile For TelePresence Conferencin
DTMF Signaling Method*
No Preference
Normalization Script
Normalization Script
< None >
Enable Trace
Parameter Name
Parameter Value
1

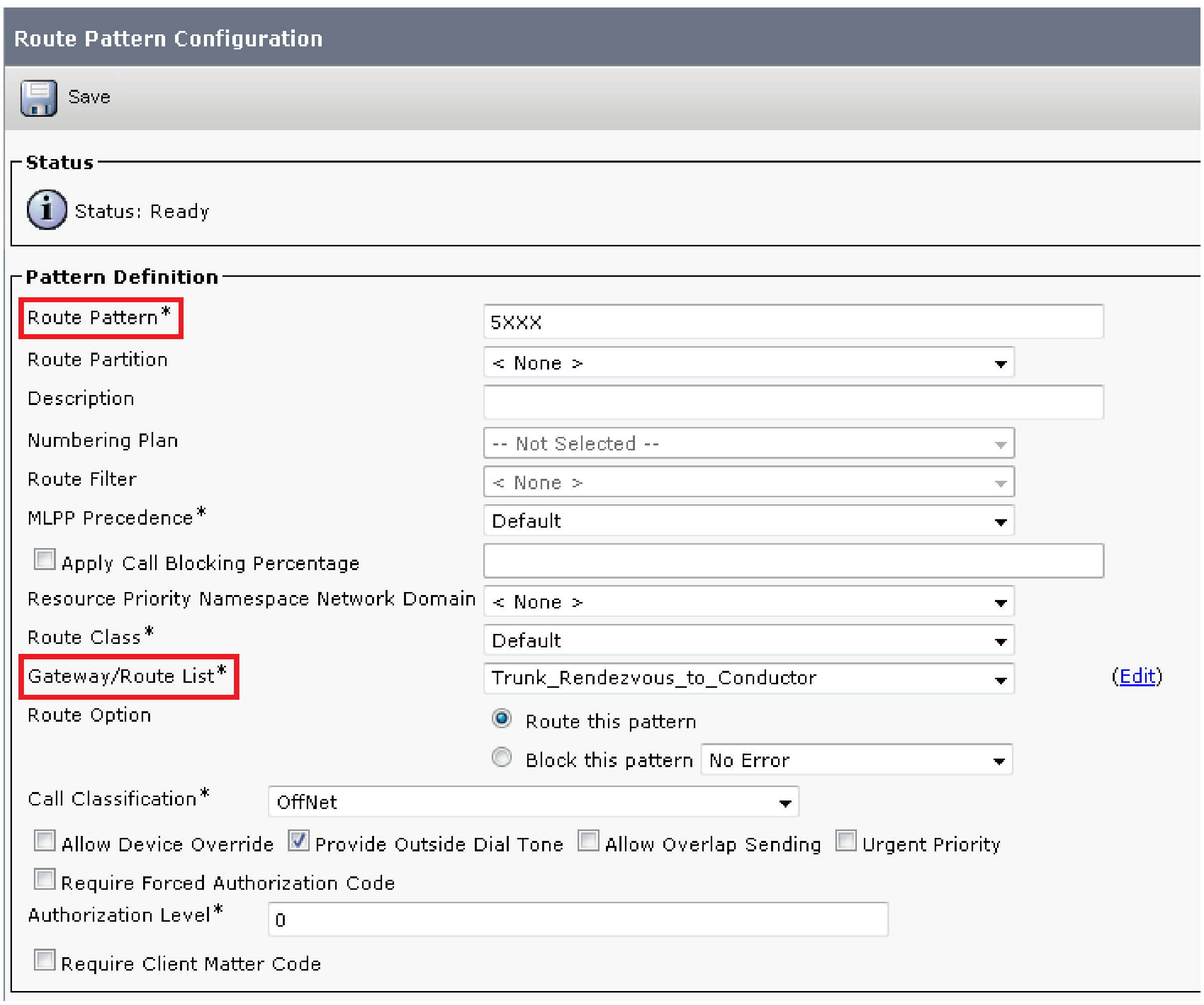
6. Click **Save**.
7. Click **Reset**.

Task 32: Adding a route pattern to match the SIP trunk to TelePresence Conductor for rendezvous meetings

To configure a route pattern to match the SIP trunk 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:

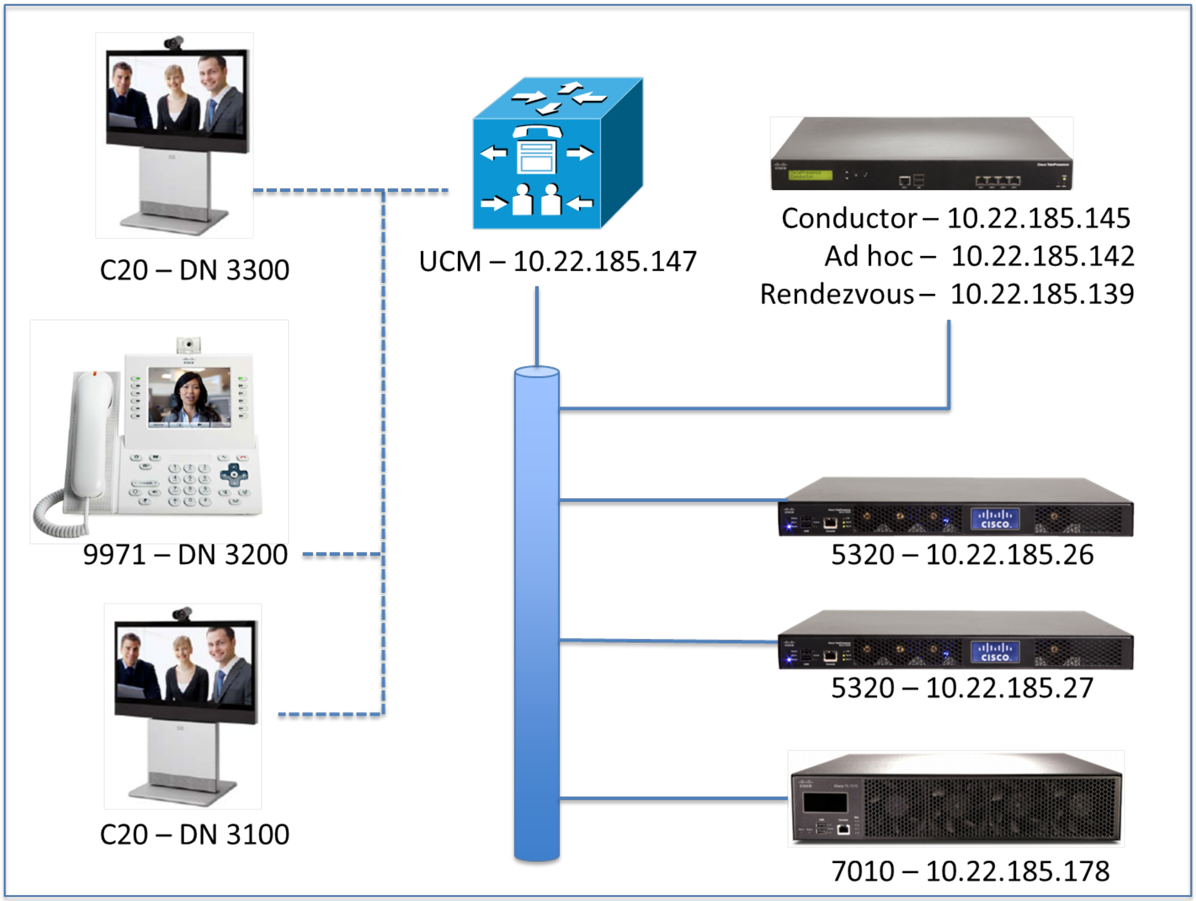
Route Pattern	Enter a route pattern to match against the destination string.
Gateway/Route List	Select the trunk created in Task 31: Adding a SIP trunk to TelePresence Conductor for rendezvous conferences (and to receive TelePresence Conductor out-dialed calls) [p.43].

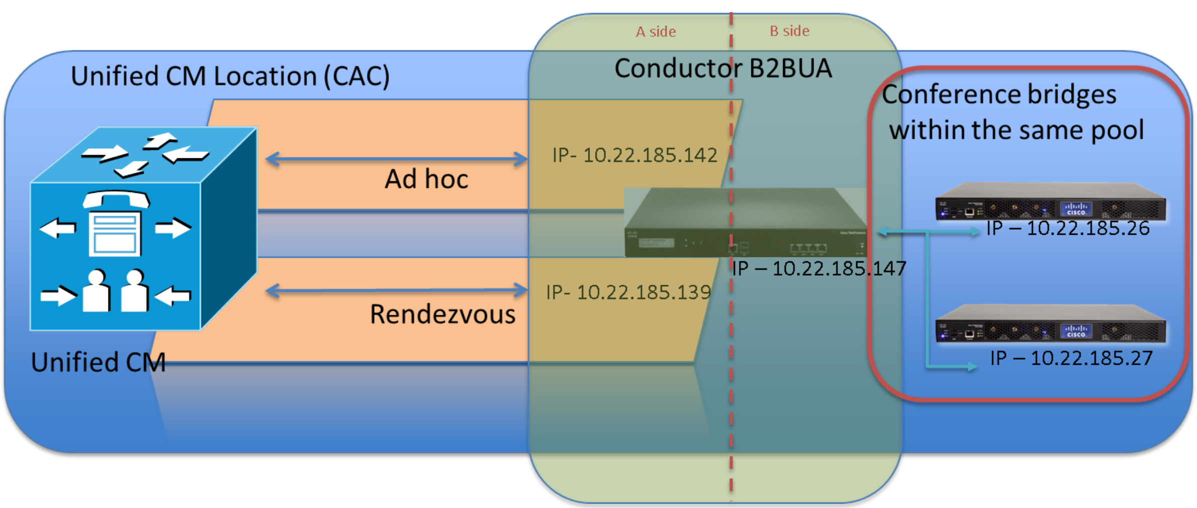


4. Click **Save**.

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:

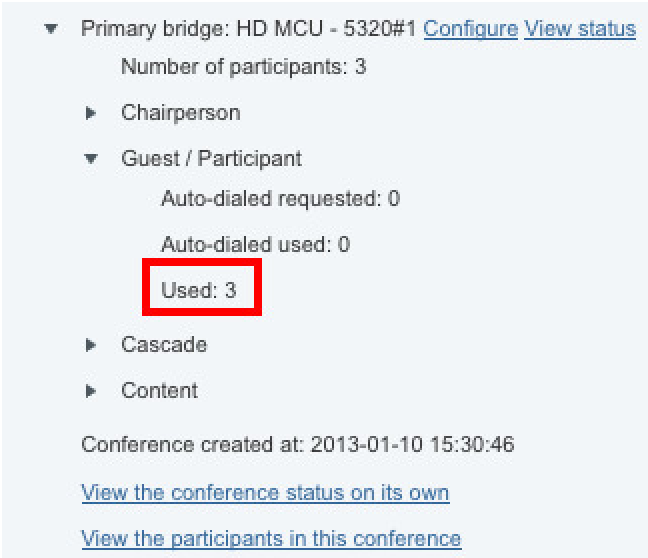




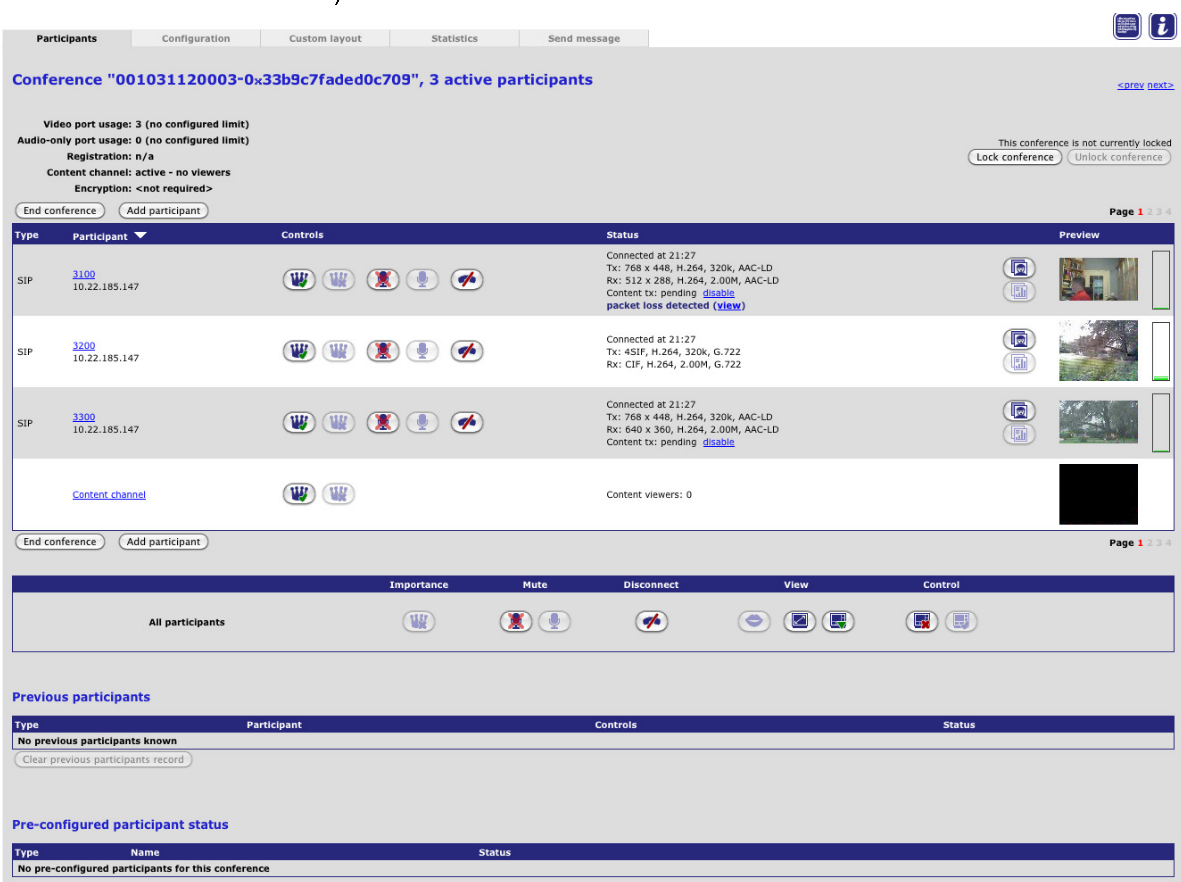
Creating an ad hoc meeting

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 the 9971 dial 3100. Verify a video and audio session is established between the 9971 and the second C20.
2. From the 9971, press the conference button and dial 3300. Verify a video and audio session is established between the 9971 and the first C20. Also note that the call between the 9971 and second C20 has been put on hold.
   Note: At this point the TelePresence Conductor is not involved.
3. From the 9971 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**.



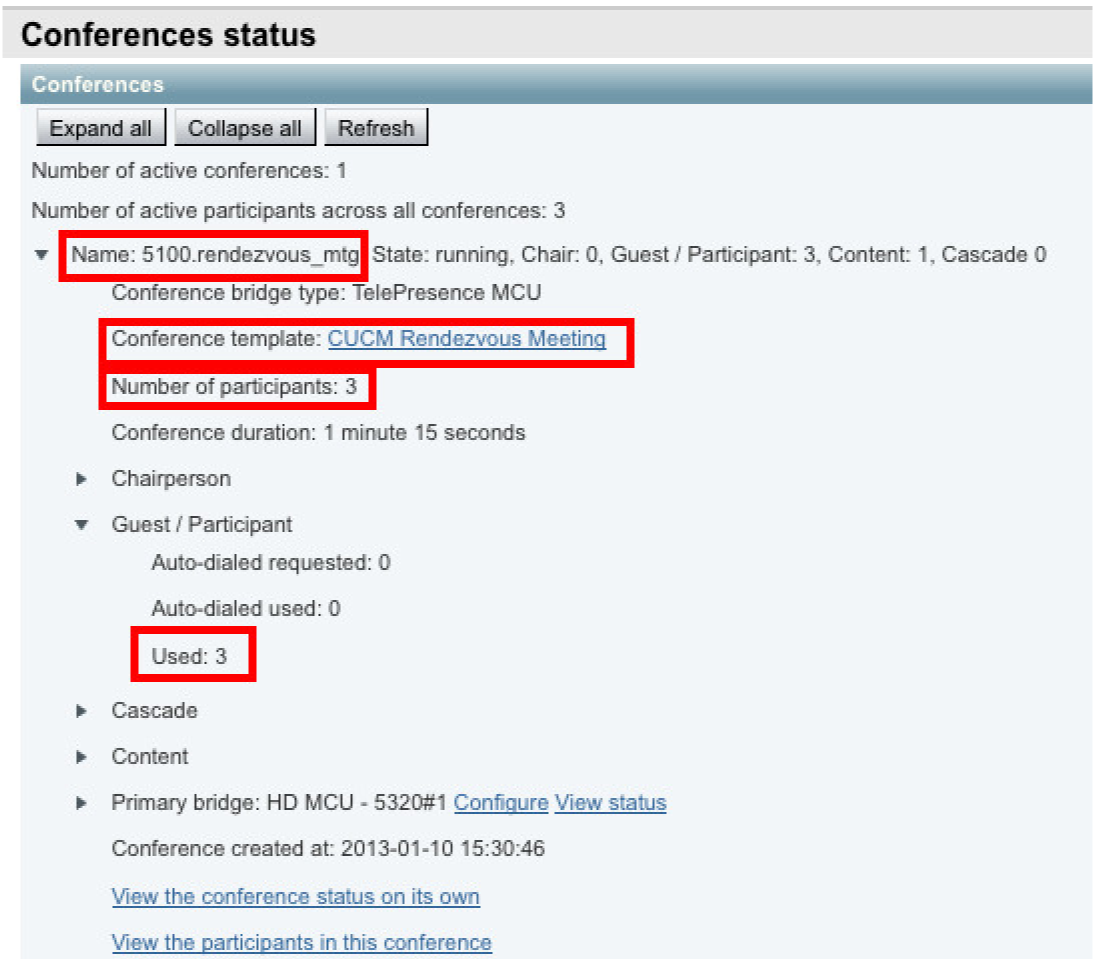
5. To verify the established call on the TelePresence MCU, go to the **Conference Status** page (**Conferences** on the main tab).

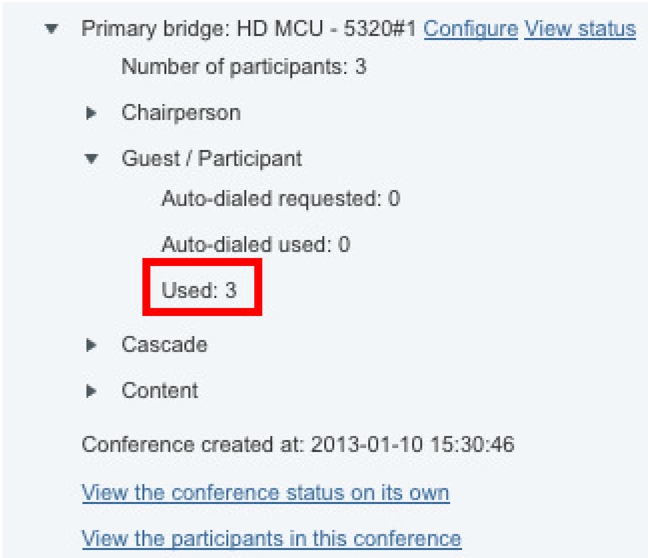


Creating a rendezvous meeting

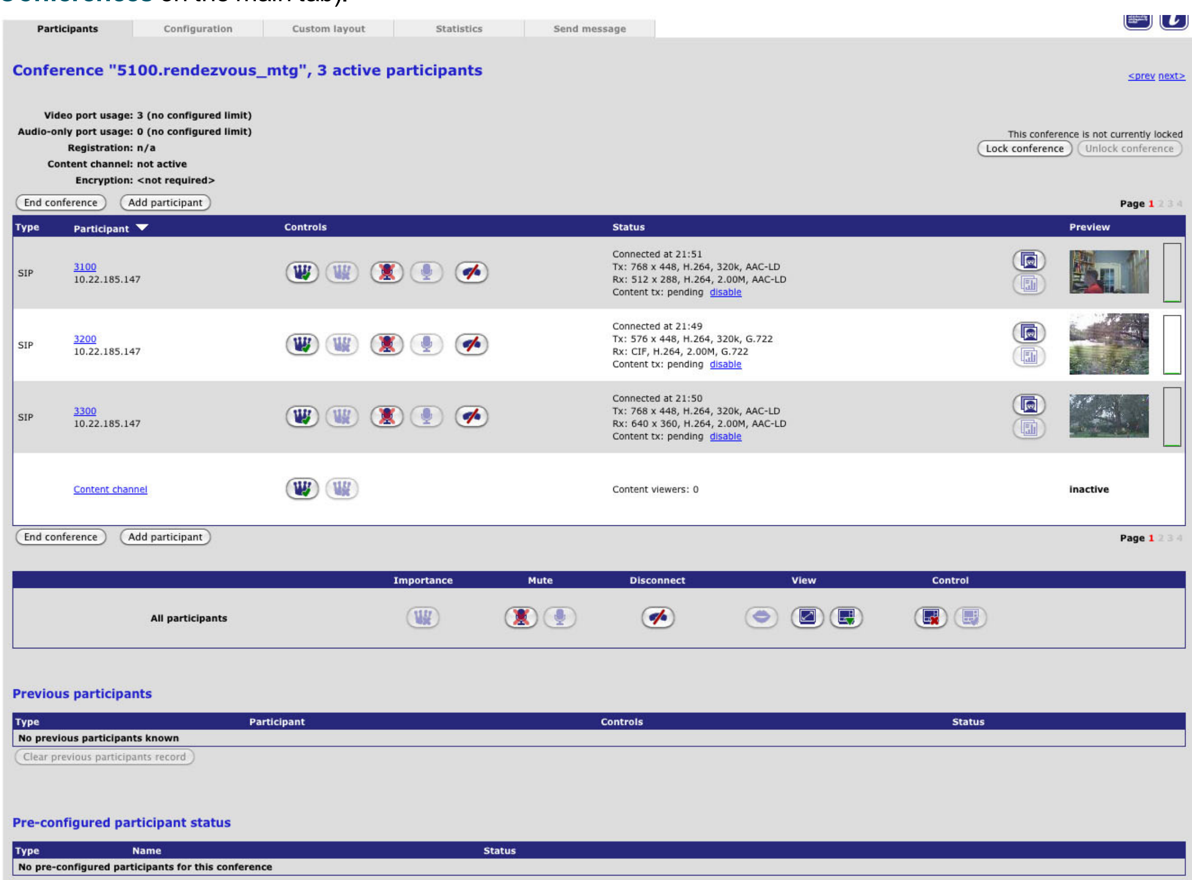
To test that two or more Unified CM-registered endpoints can join a rendezvous HD conference that is based on a TelePresence Conductor template with a type of *Meeting*, perform the following steps:

1. From the 9971 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 first C20 dial 5100. Verify a video and audio session is established between the first C20 and the TelePresence MCU.
3. From the second C20 dial 5100. Verify a video and audio session is established between the second C20 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**.





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 ports 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 chairperson ports to be reserved by 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.

For this version of the TelePresence Conductor cascading is only supported on TelePresence MCUs, not on TelePresence Servers.

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.

Note: a system backup can only be restored to the peer from which the backup was taken.

For more information see *Cisco TelePresence Conductor Administrator Guide* (D14826) or the TelePresence Conductor's online help.

Troubleshooting

Tracking a conference on the TelePresence Conductor

Event log

To see all events associated with a particular conference alias (i.e. across multiple individual conferences) 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.

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. On the 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*
   - **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** 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.
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.59].

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 MCU, verify how the conference bridge will dial the auto-dialed participant and perform the relevant steps:

Method of dialing auto-dialed participant	Configuration to verify
SIP via Unified CM	On the TelePresence Conductor go to **Conference configuration > Locations** and verify that • the **Conference type** is *Rendezvous* or *Both* • the **SIP trunk settings for out-dial calls** are set correctly to route the auto-dialed participant back to Unified CM. On the TelePresence MCU go to **Settings > SIP** and ensure the conference bridge is not registered to a SIP Proxy by having the **SIP registrar usage** field set to *Disabled*.
SIP via a proxy	On the TelePresence MCU • go to **Network > Services** and verify that **SIP (TLS)** is ticked • go to **Settings > SIP** and verify that the TelePresence MCU has the correct **SIP proxy address** defined and **Outgoing transport** set to *TLS* • check that the TelePresence MCU is registered to the SIP proxy • check that the TelePresence MCU can make outbound calls via that proxy

H323 via a gatekeeper	On the TelePresence MCU
	• go to **Network > Services** and verify that **Incoming H.323** is ticked
	• go to **Settings > H323** and verify that
	  ○ **H.323 gatekeeper usage** is *Enabled*
	  ○ **Gatekeeper address** contains the correct address
	  ○ **H.323 ID to register** is correct
	• check that the TelePresence MCU is registered to the H323 gatekeeper
	• check that the TelePresence MCU can make outbound calls via that gatekeeper

4. 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*.

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

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 **Provision for multiscreen** drop-down menu, select *Yes*.
4. Click **Save**.

Only one screen of a 3-screen CTS endpoint is used

CTS endpoints with three screens must be provisioned 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 **Chairperson quality** or **Guest quality** drop-down menu (for Lectures), select the appropriate multi-channel audio quality setting.
6. Ensure that **Provision for multiscreen** is set to *Yes*.
7. Click **Save**.

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**.

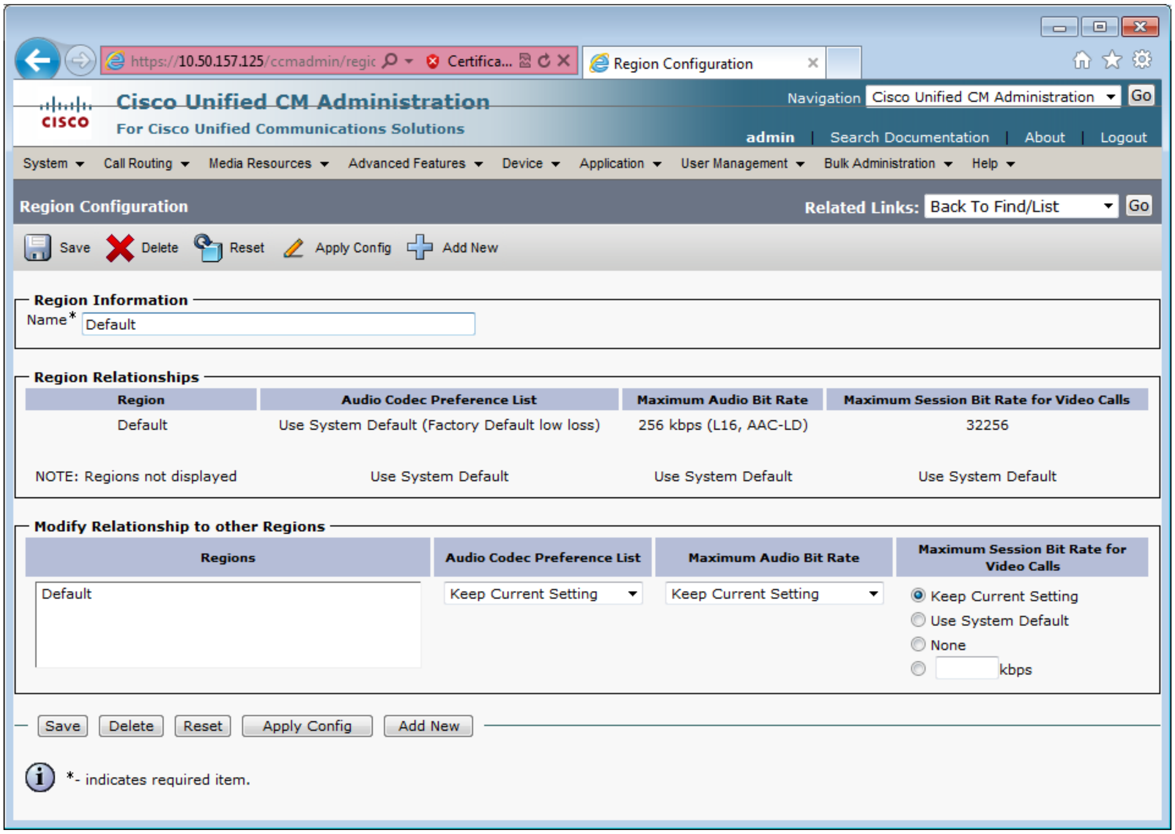
To resolve this issue on Unified CM version 8.6.2:

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.

Auto-dialed participant joins the conference before the PIN is provided to the TelePresence MCU

A conference template on the TelePresence Conductor is configured to require a PIN on the TelePresence MCU and it has an auto-dialed participant associated with it.

An endpoint dials into a conference that is based on the conference template and hangs up before the user provides a PIN. In this case the auto-dialed participant is called and joins into the conference even though there are no participants in the conference. The call to the auto-dialed participant stays up until the max timer is reached.

To work around this issue (for a TelePresence MCU version 4.4 or later) and cause the conference bridge to delay calling the auto-dialed participant until at least one participant has entered the PIN and successfully joined the conference:

1. On the TelePresence Conductor, go to **Conference configuration > Conference templates** and select the relevant conference template.
2. In the **Advanced parameters** section click **Edit**.
3. Tick the first box next to **Custom parameters** and enter the following text into the adjacent text-box: **`{"preconfiguredParticipantsDefer":true}`**
4. Click **Save** on the **Advanced template parameters** page.
5. Click **Save** on the **Conference templates** page.

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.

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.

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

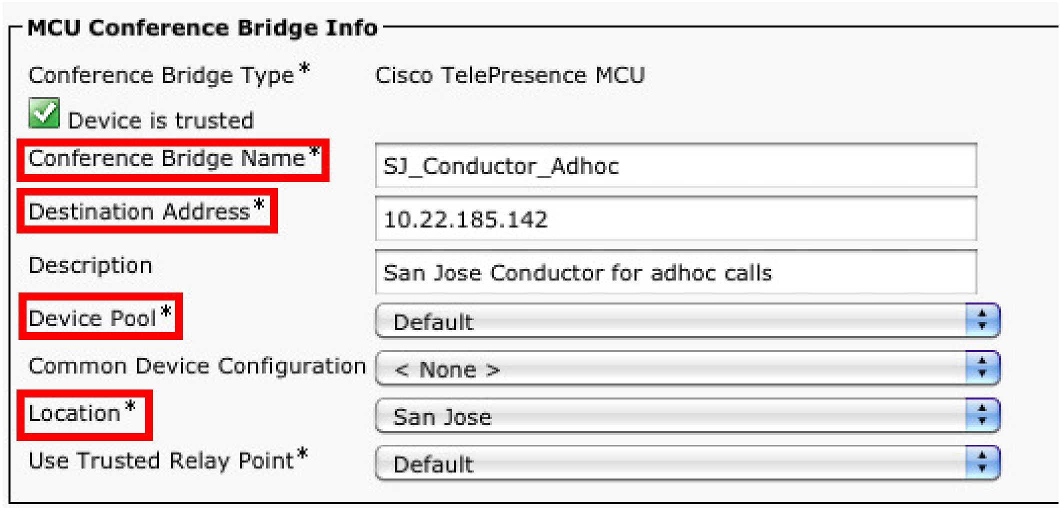
This section covers the differences between version 8.6.2 and version 9.0 of Unified CM when configuring it for use with the TelePresence Conductor. The individual steps in the section Configuring Unified CM [p.33] are from a Unified CM version 9.0 and should be replaced with the relevant steps from this appendix for Unified CM version 8.6.2 configuration.

Adding TelePresence Conductor to Unified CM for ad hoc conferences

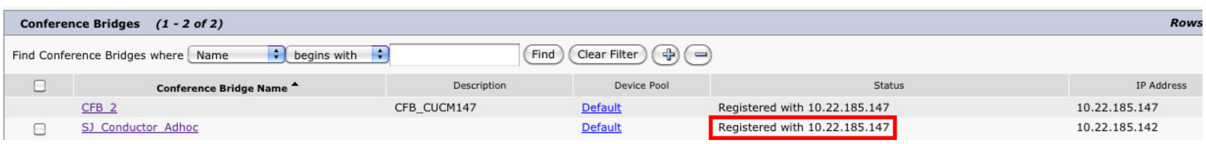
For Unified CM version 8.6.2, replace Task 27: Adding the TelePresence Conductor as a Conference bridge to Unified CM for ad hoc conferences [p.36] with the following:

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: 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.
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. Go to **Device > Trunk** and select the SIP trunk used for rendezvous conferences.
10. In the **Normalization script** section towards the bottom of the page, from the drop-down list select the script you have just added (**telepresence-conductor-interop**).
11. For Unified CM 9.0 only, go to **Media Resources > Conference Bridge** and select the conference bridge used for ad hoc conferences.
12. In the **Normalization Script Info** section towards the bottom of the page, from the drop-down list select the script you have just added (**telepresence-conductor-interop**).

Appendix 3: 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 4: Personal 4-Way Multiparty Conferencing

About Personal 4-Way Multiparty

Personal 4-Way Multiparty provides a license for a named user to host a video conference with up to three other participants. It enables personal video conferencing for users who need to hold frequent impromptu discussions with small groups of colleagues.

A named user is entitled to host a four-party video conference, including:

- Personal MeetMe address
- Ad-hoc conferences
- Video resolution up to HD

Note: only deployments using TelePresence Server conference bridges support this feature.

Configuration requirements

- The maximum number of TelePresence connections allowed for a personal multiparty video conference must be set to four.
- The video quality level for a personal multiparty video conference must be set to HD or lower in the TelePresence Conductor's conference template.
- The content quality level for a personal multiparty video conference must be set to 1280 x 720p 5fps or lower in the TelePresence Conductor's conference template.
- The number of conference aliases for MeetMe or personal multiparty conferences should not exceed the number of licenses.
- The named host must be present for the multiparty video conference to begin.

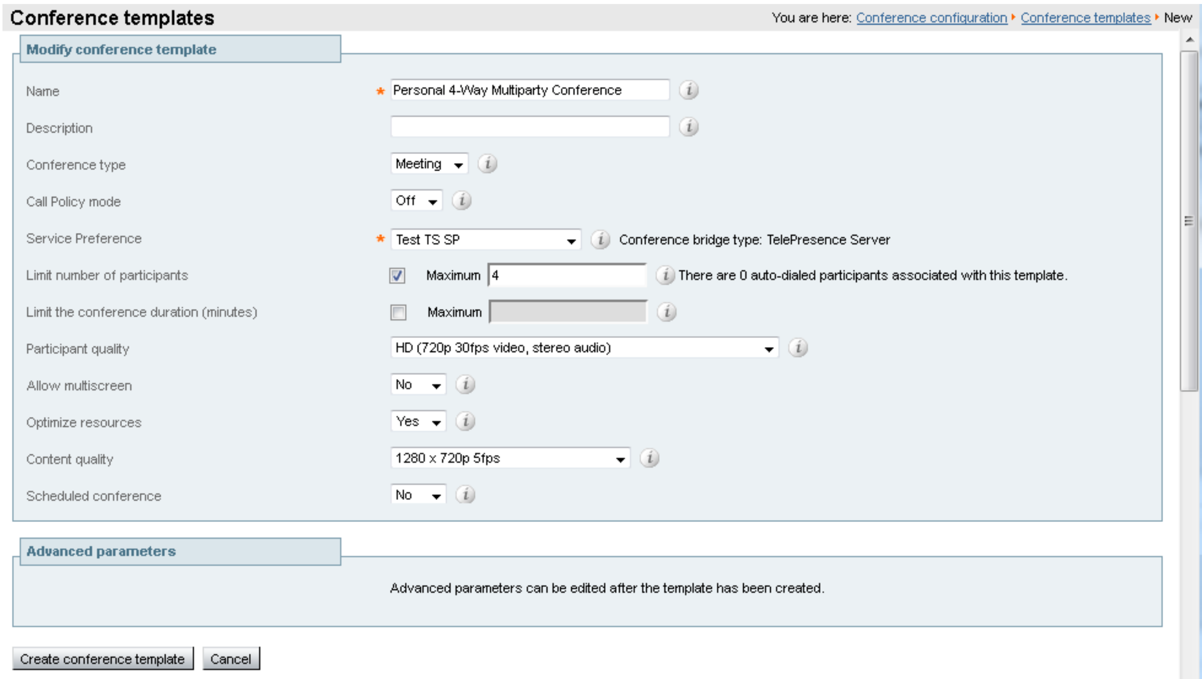
Configuration tasks

Task 1: Creating a conference template in TelePresence Conductor

To configure support for Personal 4-Way Multiparty, you must set specific parameters in the conference template in TelePresence Conductor.

To create a new conference template for Personal 4-Way Multiparty:

1. On TelePresence Conductor go to **Conference configuration > Conference templates**.
2. Click **New**.
3. Set the **Conference type** to *Meeting*.
4. Select a **Service Preference** containing conference bridges of type TelePresence Server.
5. Tick the box for **Limit number of participants** and in the **Maximum** field, enter *4*.
6. Set the **Participant quality** to *HD (720p 30fps video, stereo audio)* or lower.
   Note: Full HD is not supported with Personal 4-Way Multiparty.
7. Set the **Content quality** to *1280 x 720p 5fps*.



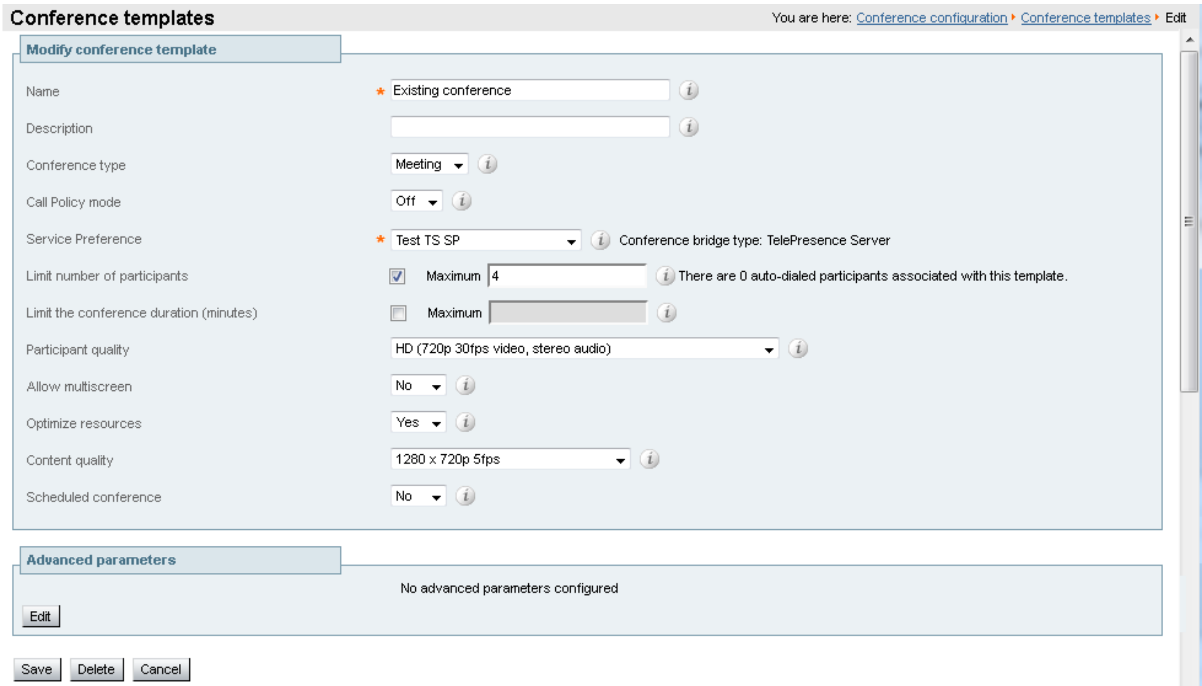
8. Click **Create conference template**.

Task 2: Updating existing conference templates in TelePresence Conductor

If you are using Personal 4-Way Multiparty all conference templates must be configured to support Personal 4-Way Multiparty.

To update all existing conference templates:

1. On TelePresence Conductor go to **Conference configuration > Conference templates**.
2. Click on the name of the conference template you wish to update.
3. Set the **Conference type** to *Meeting*.
4. Select a **Service Preference** containing conference bridges of type TelePresence Server.
5. Tick the box for **Limit number of participants** and in the **Maximum** field, enter *4*.
6. Set the **Participant quality** to *HD (720p 30fps video, stereo audio)* or lower.
   Note: Full HD is not supported with Personal 4-Way Multiparty.
7. Set the **Content quality** to *1280 x 720p 5fps*.



8. Click **Save**.
9. Repeat the steps above for all other existing conference templates.

Document revision history

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

Revision	Date	Description
09	March 2014	Removed configuration task on Unified CM within Personal 4-Way Multiparty Conferencing section.
08	February 2014	Added appendix for Personal 4-Way Multiparty and corrected link to UCM normalization script.
07	August 2013	Updated for release XC2.2
06	August 2013	Corrected the recommendation for uploading server certificates and how to troubleshoot auto-dialed participants not being called
05	May 2013	Updated for release XC2.1
04	April 2013	Corrected the SIP configuration for MCUs
03	March 2013	Added information about lack of cascading support in ad hoc conferences
02	February 2013	Restructured the document and updated some screen shots
01	December 2012	Initial release.