Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager

Deployment Guide

XC2.2
Unified CM 8.6.2 and later

D15000.05

Revised December 2013

Contents

Introduction

About this document

This document assumes that a standalone Cisco TelePresence Conductor integration with Cisco Unified Communications Manager (Unified CM) ad hoc and rendezvous calls has been set up according to the *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*. This guide provides details on how to:

- Extend the TelePresence Conductor integration with Unified CM to a cluster of TelePresence Conductors for ad hoc and rendezvous calls.
- Back up a TelePresence Conductor cluster.
- Remove a TelePresence Conductor peer from Unified CM for ad hoc and rendezvous calls.
- Upgrade a TelePresence Conductor cluster.

Further reading

For details on how to integrate a TelePresence Conductor cluster with Cisco VCS see either *Cisco TelePresence Conductor Clustering with Cisco VCS (Policy Server) Deployment Guide* or *Cisco TelePresence Conductor Clustering with Cisco VCS (B2BUA) Deployment Guide* depending on the type of Cisco VCS deployment used.

For more details on Unified CM not covered in this deployment guide, including how to implement a Unified CM or Unified CM cluster please reference the documentation on Cisco.com under the Cisco Unified Communications Manager, http://www.cisco.com/en/US/products/sw/voicesw/ps556/index.html.

For details on how to deployUnified CM, TelePresence Conductor, and the Conference bridges in an end-to-end secure network see *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.

About TelePresence Conductor clustering

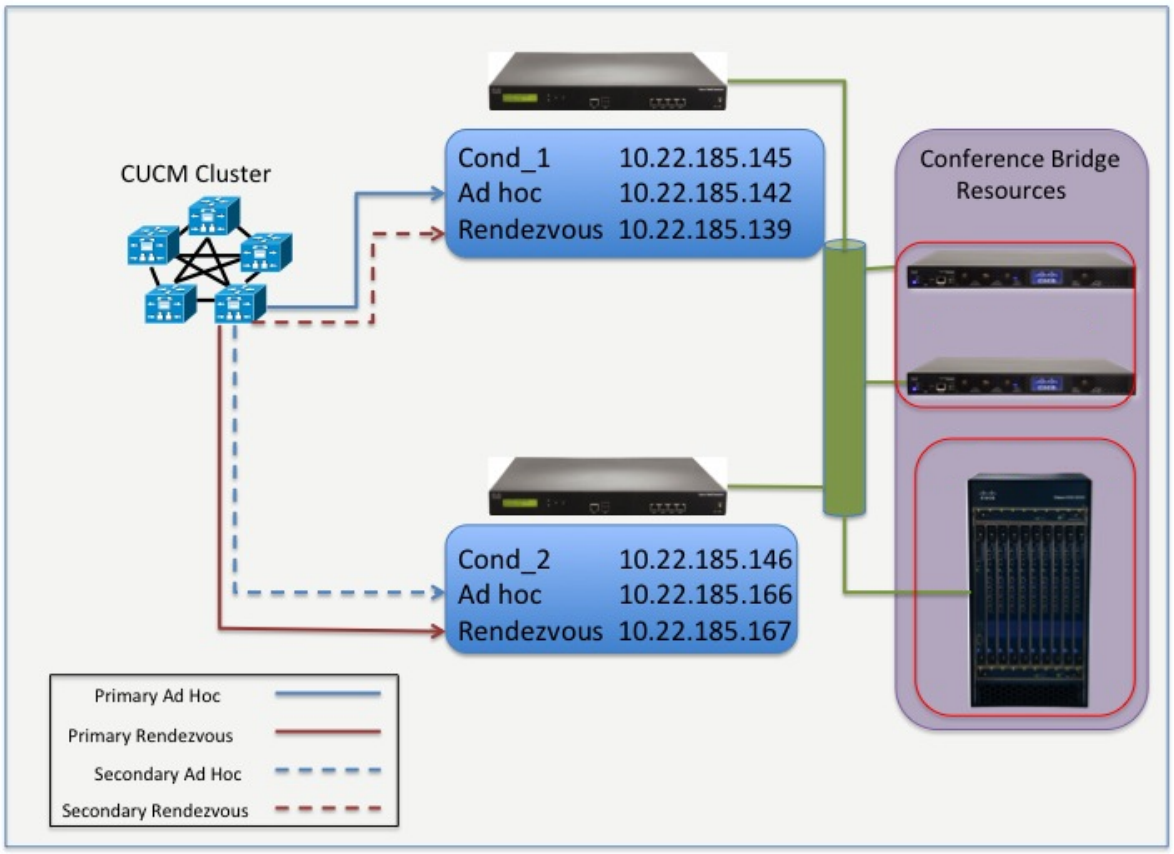
Clusters of TelePresence Conductors are used to provide redundancy in the rare case of the failure of an individual TelePresence Conductor (for example, due to a network or power outage). Each TelePresence Conductor is a peer of the other TelePresence Conductors in the cluster. Each peer knows about all conferences. It can add callers to conferences created by other peers and it can create conferences that it or other peers can add calls to.

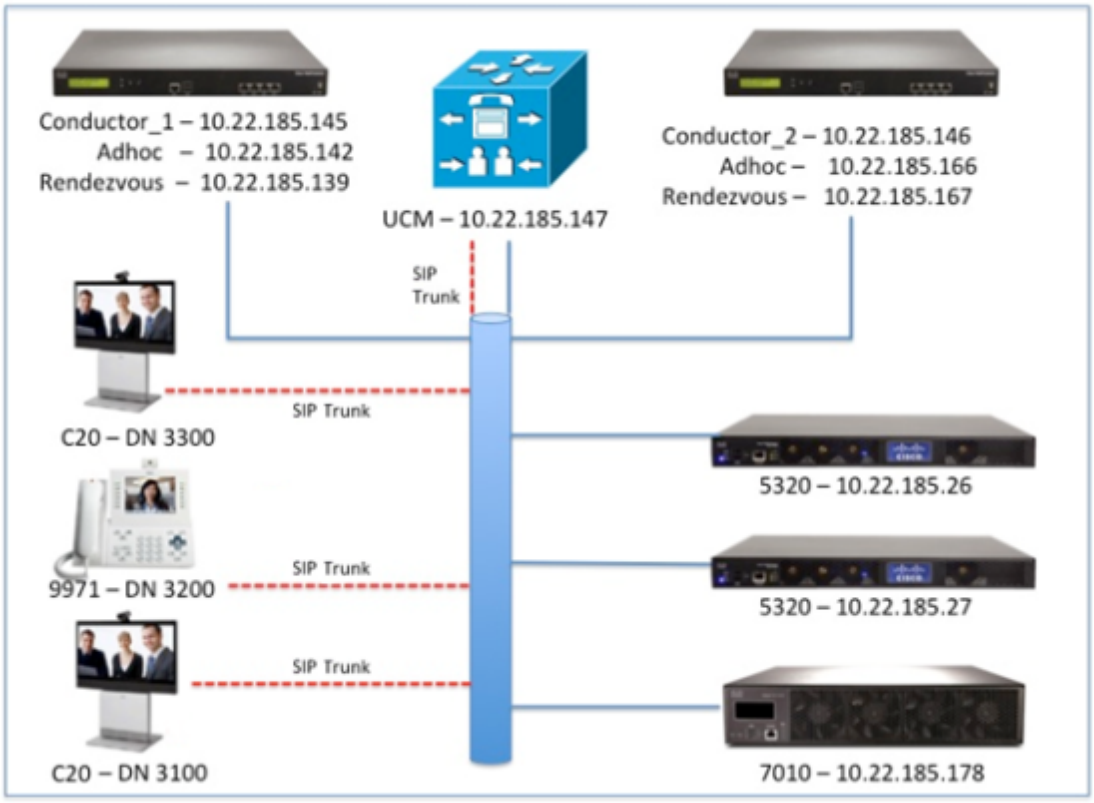
The process to integrate a cluster of TelePresence Conductors depends upon whether the TelePresence Conductor cluster is communicating with a Cisco Video Communication Server (Cisco VCS) or a Cisco Unified Communications Manager (Unified CM). This document explains the process of creating and integrating a cluster of TelePresence Conductor peers with Unified CM.

To handle a cluster of TelePresence Conductor peers the Unified CM will be configured to have direct links to all the TelePresence Conductors in the cluster. If one TelePresence Conductor fails, Unified CM will then route the call to a different TelePresence Conductor for call completion. This process is transparent to the user and offers virtually no interruption in service.

Example network deployment

This document uses the example network shown in the diagrams below as the basis for the deployment configuration described. During configuration, refer back to these diagrams to see the relationship between a Unified CM cluster and a redundant set of TelePresence Conductors.





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. This version of the TelePresence Conductor 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 Cisco Jabber Video for TelePresence, desktop endpoints such as the 9971 and EX90, or room systems such as the MX300.

Creating a TelePresence Conductor cluster

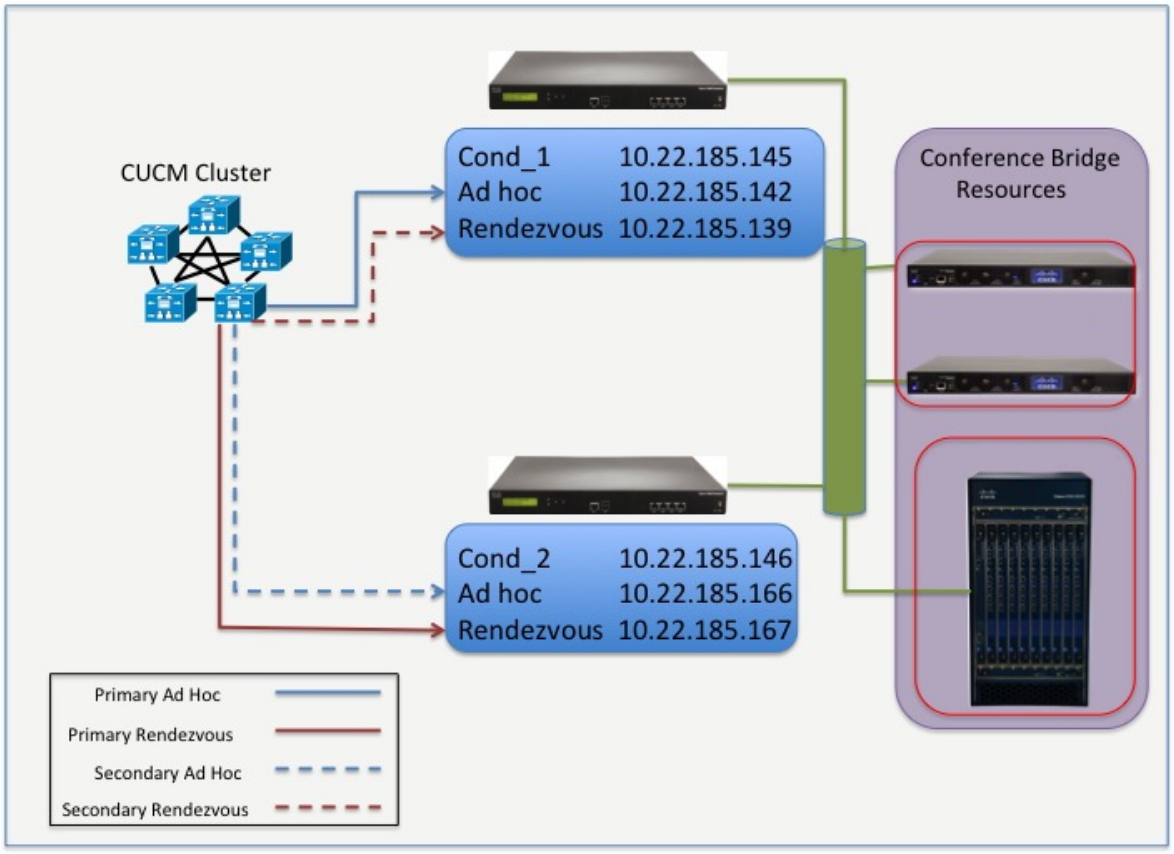
Prerequisites

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

- A standalone TelePresence Conductor has been configured to work with a Unified CM and at least one conference bridge according to the *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.
- Every TelePresence Conductor to be used in the cluster must be running the same version of XC software. TelePresence Conductor clustering with Unified CM is supported in version XC2.0 and later.
- If using full capacity TelePresence Conductors, up to three peers can be clustered and all peers must be full capacity versions.
- If using TelePresence Conductors with the option key supporting up to 50 concurrent call sessions installed, up to two peers can be clustered and both peers must have the same option key installed.
- The Unified CM must be running version 8.6.2 or later (version 9.1.1 or later is highly recommended).
- Enough unique IP addresses are available to configure each TelePresence Conductor peer with addresses to fulfill the requirements for ad hoc and rendezvous type call configuration.
  Each cluster peer 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.
- All TelePresence Conductor cluster peers must be configured to use either the same NTP servers, or NTP servers that are very closely synchronized. The NTP servers can be viewed and configured on the **Time** page (**System>Time**).
- All TelePresence Conductor cluster peers must be located closely enough so that there is a maximum round trip time of 30 milliseconds between any pair of cluster peers.
- Every conference bridge in use by TelePresence Conductor must be reachable by every TelePresence Conductor peer over HTTP/HTTPS and SIP TLS.
- For information on the ports that must be open between the TelePresence Conductor peers see Appendix 2: IP ports and protocols [p.37].

Integration overview

As part of a solid network design, implementation of redundancy within the system is critical. This can be achieved for a Unified CM and TelePresence Conductor integration using additional TelePresence Conductors configured as additional options for Unified CM to use to place ad hoc and rendezvous calls. The diagram below depicts a resilient scenario in a single site design. We recommend that when configuring the Unified CM and TelePresence Conductor integration, to ensure that the primary TelePresence Conductor for ad hoc calls, **Cond_1**, is the secondary TelePresence Conductor for rendezvous calls and the opposite configuration for **Cond_2**, where it is the primary TelePresence Conductor for rendezvous calls and secondary for the ad hoc calls, or that ad hoc and rendezvous calls use round robin so that calls are load balanced across the TelePresence Conductor peers.



In a design where a single Unified CM cluster or multiple Unified CM clusters support multiple CAC locations, 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.

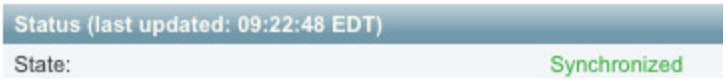
Note: for ad hoc conferences the conference bridges to use are indirectly configured by the template that is configured on the TelePresence Conductor's **Locations** page (Conference template > Service Preference > Conference bridge pools > Conference bridges). The conference bridges to use for rendezvous 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.

Configuring the TelePresence Conductor

Task 1: Checking the configuration

1. Decide which TelePresence Conductor is to be the initial peer. **The configuration of this system will be shared with all other peers as they are added to the cluster**. For the purposes of this example, we shall refer to this peer as **Conductor_1**.
   Note: if you choose an un-configured Conductor as the initial peer it will wipe the configuration of other peers as they are added.

2. Verify that no other TelePresence Conductor already has **Conductor_1**'s IP address in their clustering peers list. To do this verification:
   a. Log into every TelePresence Conductor as a user with administrator rights.
   b. Go to **System > Clustering**.
   c. Ensure that all **Peer X IP address** fields (X = 1, 2, and 3) on this page do not have **Conductor_1**'s IP address.
   If they do:
      i. Delete that Peer IP address.
      ii. Click **Save**.
      iii. Go to **Maintenance > Restart options**.
      iv. Click **Restart**.
3. Log into **Conductor_1** as a user with administrator rights.
4. Ensure that **Conductor_1** has a valid and working NTP server configured:
   a. Go to **System > Time**.
   b. In the **Status** section at the bottom of the page, the **State** should be *Synchronized*:



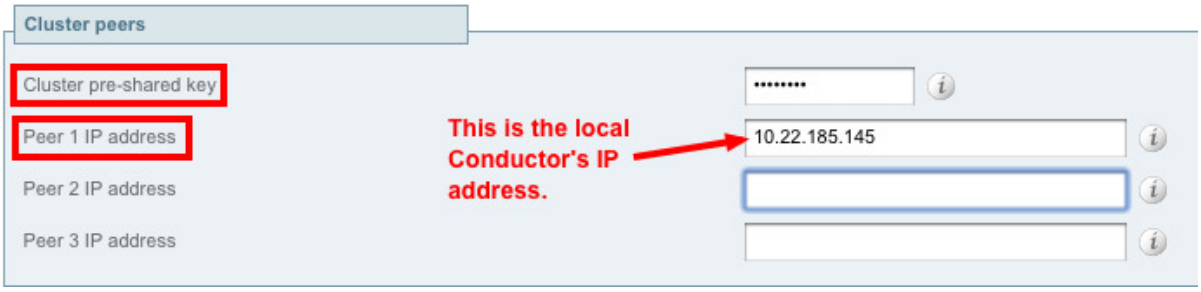
5. Ensure that **Conductor_1** has the correct DNS settings configured:
   a. Go to **System > DNS**.
   b. Ensure that **Conductor_1** has at least one valid DNS server configured.
   c. Ensure that **Conductor_1** has the correct **Domain name** and **System host name** configured: <System host name>.<domain name> = FQDN of this TelePresence Conductor.
6. Ensure that **Conductor_1** has the correct Clustering settings applied:
   a. Go to **System > Clustering**.
   b. Ensure that all **Peer X IP address** fields (X = 1, 2, and 3) on this page are blank. If not:
      i. Delete any entries.
      ii. Click **Save**.
   c. Ensure that **Conductor_1** has no **Cluster pre-shared key** configured. If there is a value in the **Cluster pre-shared key** field:
      i. Delete the entry.
      ii. Click **Save**.
      iii. Go to **Maintenance > Restart options**.
      iv. Click **Restart**.

Task 2: Creating a cluster of one peer

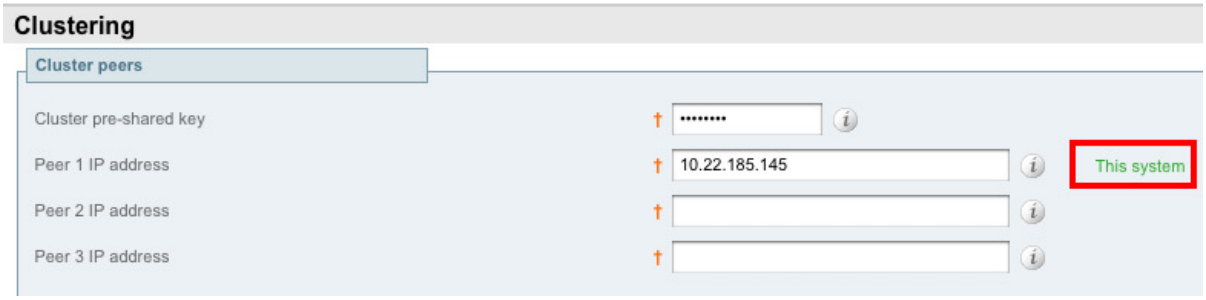
1. On **Conductor_1**, go to **System > Clustering**.
2. Enter the following values in the relevant fields:

Cluster pre-shared key	Enter a password (this will be the same for all peers).
Peer 1 IP address	Enter the IP address of this TelePresence Conductor peer, **Conductor_1** (this is the initial peer in the cluster from which the initial configuration will be replicated from to all other peers in the cluster).

Peer 2 IP address	Leave blank at this point in the configuration.
Peer 3 IP address	Leave blank at this point in the configuration.



3. Click **Save**.
4. Go to **Maintenance > Restart options**.
5. Click **Restart**.
6. Log into **Conductor_1** as a user with administrator rights.
7. Go to **System > Clustering**.
8. Verify the status of this peer. It should have **This System** in green next to the IP address.

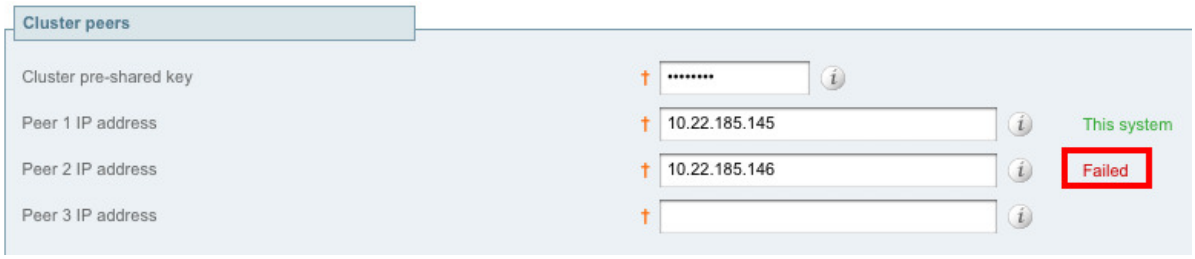


Task 3: Configuring the cluster to accept the new peer

These instructions specify how to add a second peer to the cluster. A third peer can be added in a similar manner using Peer 3 IP address, and configuring both peer 1 and peer 2 before configuring peer 3.

On the initial cluster peer (i.e. the initial peer which is configured as a cluster of one peer):

1. Log into the initial TelePresence Conductor, **Conductor_1**, as a user with administrator rights.
2. Go to **System > Clustering**.
3. In the **Peer 2 IP address** field, enter the new peer's IP address. For the purposes of this example we shall refer to this peer as **Conductor_2**.
4. Click **Save**.
5. Notice the peer's **Status** is *Failed*. This is normal for this stage of the configuration process.



6. Click **Save**.
7. Go to **Maintenance > Restart options**.
8. Click **Restart**.

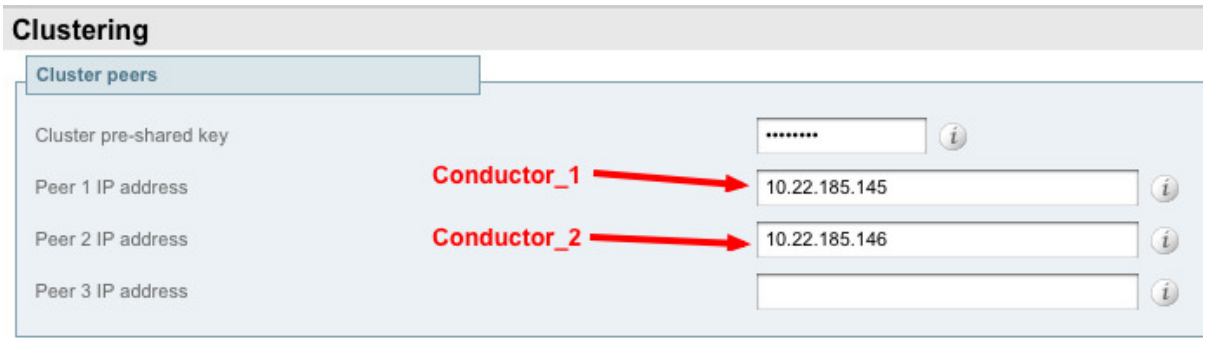
Task 4: Checking the configuration of the second peer

1. Log into the new peer, **Conductor_2**, as a user with administrator rights.
2. Ensure that **Conductor_2** has a valid and working NTP server configured:
   a. Go to **System > Time**.
   b. In the **Status** section at the bottom of the page, the **State** should be *Synchronized*:

3. Ensure that **Conductor_2** has the correct DNS settings configured:
   a. Go to **System > DNS**.
   b. Ensure that **Conductor_2** has at least one valid DNS server configured.
   c. Ensure that **Conductor_2** has the correct **Domain name** and **System host name** configured: <System host name>.<domain name> = FQDN of this TelePresence Conductor.
4. Ensure that **Conductor_2** has the correct Clustering settings applied:
   a. Go to **System > Clustering**.
   b. Ensure that all **Peer X IP address** fields (X = 1, 2, and 3) on this page are blank. If not:
      i. Delete any entries.
      ii. Click **Save**.
   c. Ensure that **Conductor_2** has no **Cluster pre-shared key** configured. If there is a value in the **Cluster pre-shared key** field:
      i. Delete the entry.
      ii. Click **Save**.
      iii. Go to **Maintenance > Restart options**.
      iv. Click **Restart**.

Task 5: Configuring the new peer to join the cluster

1. On this peer, go to **System > Clustering**.
2. In the **Cluster pre-shared key** field, enter the same password that was used for the initial peer, **Conductor_1**.
3. In the **Peer 1 IP address** field, enter the IP address of the initial peer, **Conductor_1**.
4. In the **Peer 2 IP address** field, enter the IP address of the local TelePresence Conductor, **Conductor_2**.

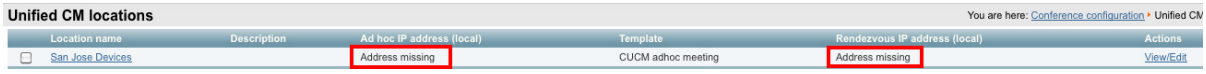


5. Click **Save**.
   Note: Ensure that the initial peer is accessible via the web and is not still restarting. If the second peer is restarted whilst the initial peer is restarting, the wrong peer may be selected as the initial peer and configuration may be lost.
6. Go to **Maintenance > Restart options**.
7. Click **Restart**.
8. Log back into **Conductor_2** as a user with administrator rights.
9. Go to **System > Clustering**.
10. Verify the **Status** of each peer. It should have **This system** in green next to this system's IP address and show **Active** for the other peer.

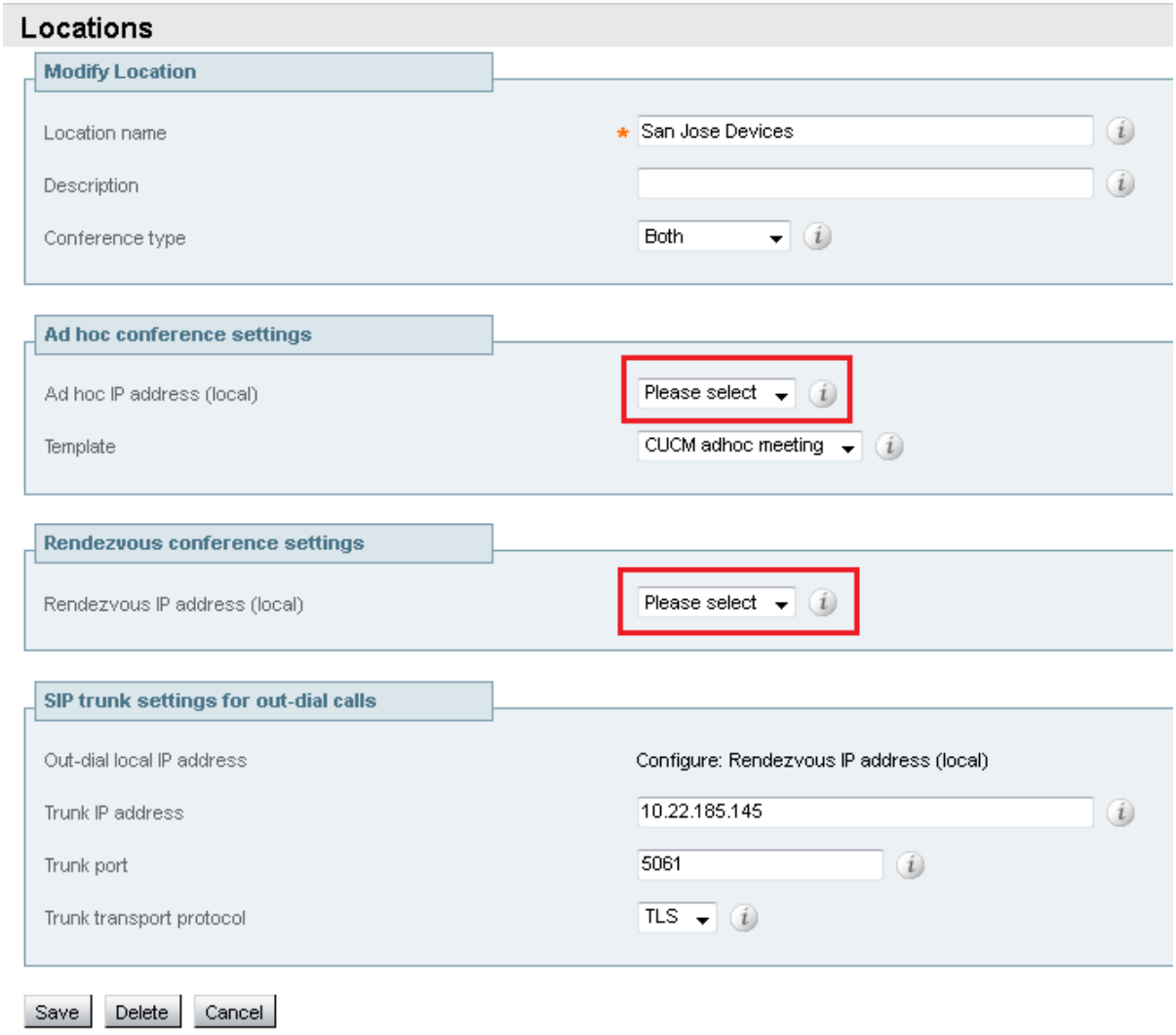
Task 6: Configuring the Locations on the peer.

As a part of the clustering process the configuration of Locations, conference aliases, conference templates, Service Preferences and conference bridges are replicated. The Location's IP address, however, needs to be configured on peer **Conductor_2**.

1. Log into the new peer, **Conductor_2**, as a user with administrator rights.
2. Go to **Conference configuration > Locations**.
3. Click **View/Edit** next to the existing location name. Also notice this location says *Address Missing* under the IP address fields. This is because a unique local IP address needs to be associated with these types of calls on this TelePresence Conductor.



4. Under the **Ad hoc** section, select the IP address from the drop-down list.
5. Under the **Rendezvous** section, select the IP address from the drop-down list.



6. Click **Save**.
7. Verify the proper IP addresses were saved and assigned to the appropriate type of calls.

8. Repeat for each Location configured.

Configuring Unified CM for ad hoc conferences

Task 7: Adding the secondary TelePresence Conductor as a bridge to the Unified CM for ad hoc conferences

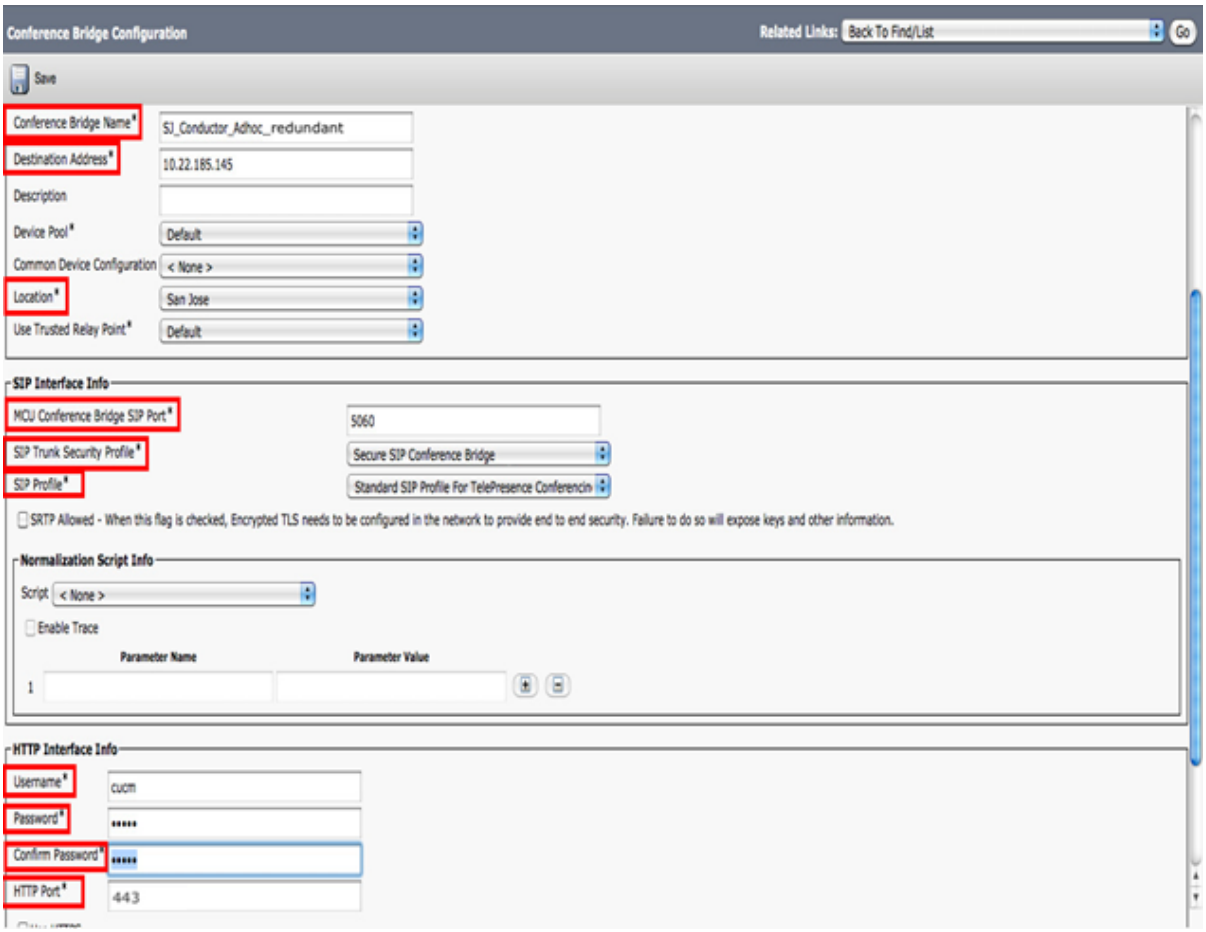
Note: The instructions in this step are for Unified CM version 9.0 or later. For version 8.6.2 go to Appendix 1: Unified CM version 8.6.2 configuration [p.35]

To configure Unified CM version 9.0 or later with TelePresence Conductor:

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:

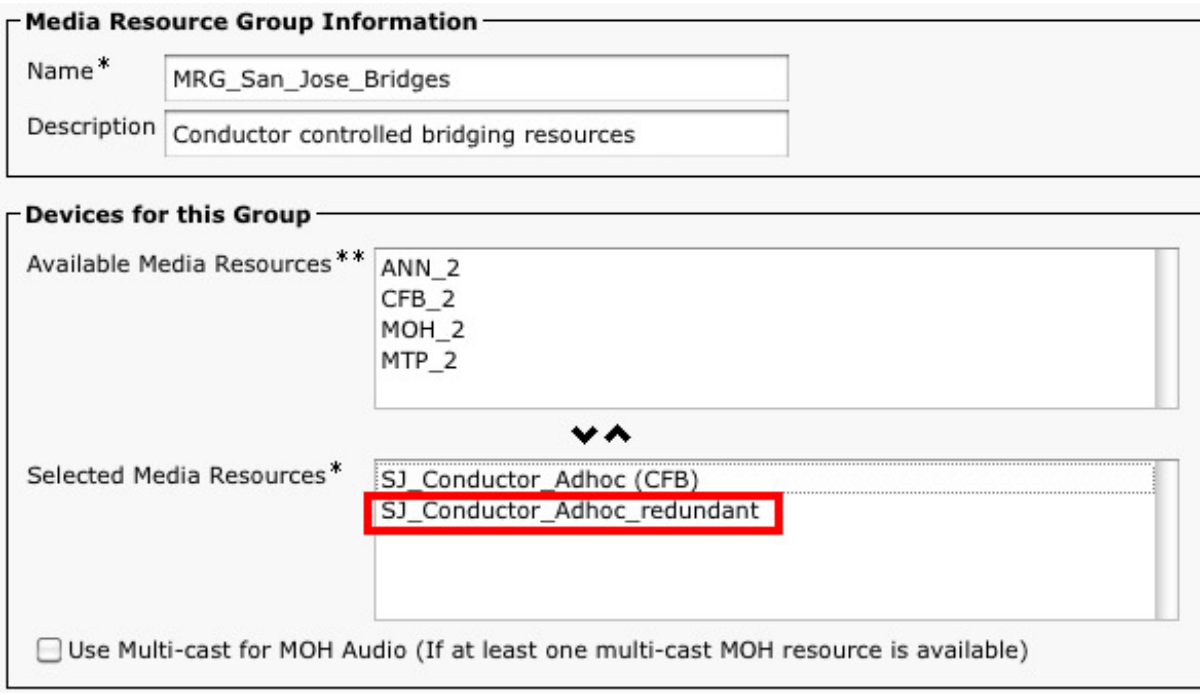
Conference Bridge Type	Select *Cisco TelePresence MCU*
Conference Bridge Name	Enter the TelePresence Conductor's Name
Destination Address	Enter the TelePresence Conductor's IP address
Device Pool	Select the appropriate pool
MCU Conference bridge SIP port	Modify the SIP listening port, if appropriate for your design, otherwise leave the default.
SIP Trunk Security Profile	Select *Secure SIP Conference Bridge*
SIP Profile	Select *Standard SIP Profile for TelePresence Conferencing*
Location	Select the appropriate location
Username	Enter the username of the TelePresence Conductor administration user. 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'.



Task 8: Adding the secondary TelePresence Conductor to an MRG and MRGL for ad hoc conferences

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 **Find** to list the Media Resource Groups.
3. Click on **MRG_San_Jose_Bridges**.
4. Move the TelePresence Conductor media bridge (the conference bridge configured in Task 7: Adding the secondary TelePresence Conductor as a bridge to the Unified CM for ad hoc conferences [p.13]) down to the Selected Media Resources box. Make sure this conference bridge is the last bridge in the list as it is the redundant TelePresence Conductor.



5. Click **Save**.

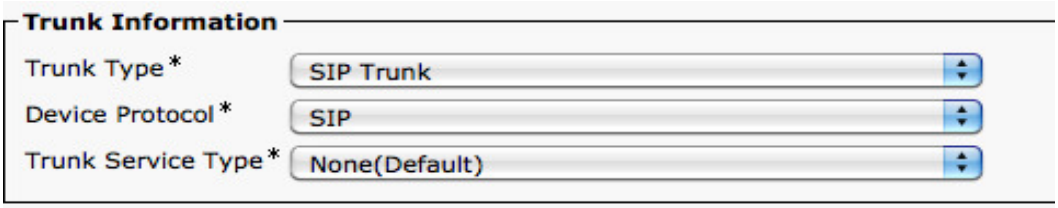
Configuring Unified CM for rendezvous conferences

Task 9: Adding a SIP trunk for the secondary TelePresence Conductor for rendezvous conferences

To configure a SIP trunk to the secondary 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, leave other fields as their default values:

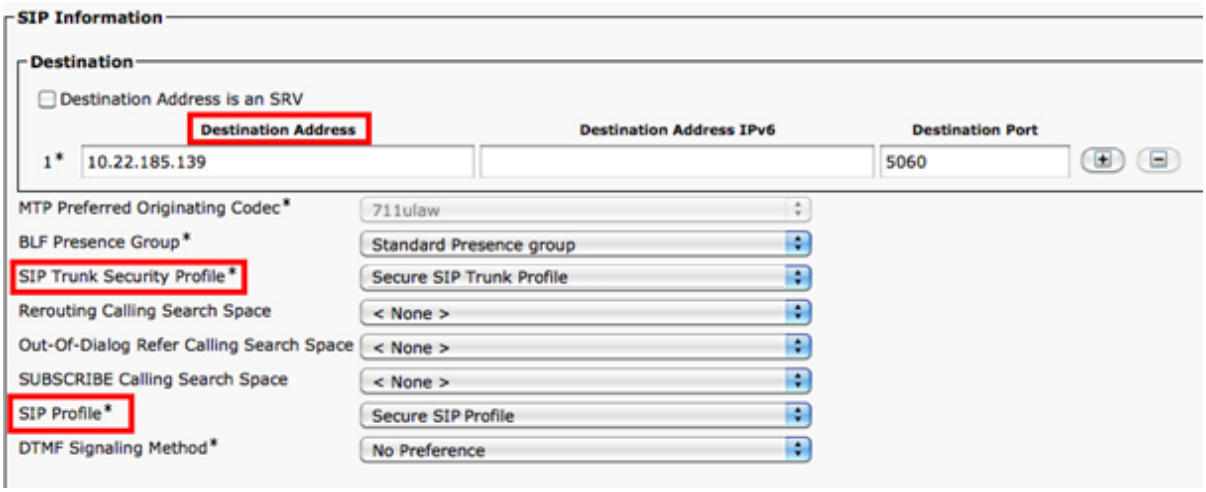
Trunk Type	Select *SIP Trunk*
Device Protocol	This should change to SIP with the trunk type selection



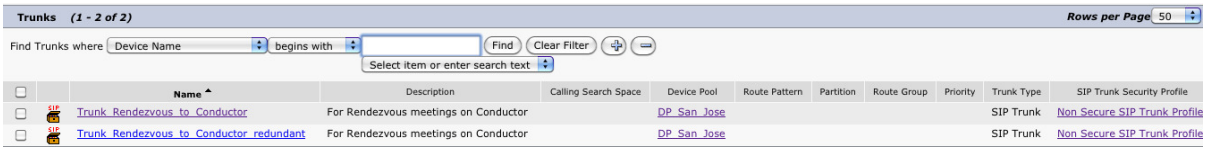
4. Click **Next**.

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

Device Name	Enter a trunk name
Location	Select the appropriate Location from the drop-down list
Device Pool	Select the appropriate Device Pool
Destination Address	Enter the IP address of **Conductor_2**'s ad hoc Location. This IP address is the one configured on the TelePresence Conductor's **Locations** page (**Conference configuration > Locations**) in the **Ad hoc conference settings** section.
SIP Trunk Security Profile	Select the *Secure SIP Trunk Profile* from the drop-down list
SIP Profile	Select the *Secure SIP Profile* from the drop-down list



6. Click **Save**.
7. Click **Reset**.
8. There should now be two trunks set up to route rendezvous calls to the primary and secondary TelePresence Conductors.



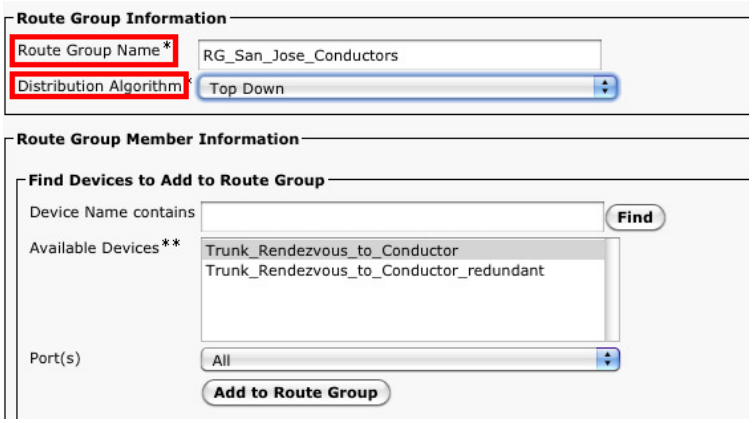
Task 10: Adding a route group for the SIP trunks

To configure a route group to use the SIP trunks to the TelePresence Conductor for rendezvous calls:

1. Go to **Call Routing > Route/Hunt > Route Group**.
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 Group Name	Enter a route group name
Distribution Algorithm	Select *Top Down*



4. Under the Route Group Member section, highlight **Trunk_Rendezvous_to_Conductor** and click **Add to Route Group**.
5. Under the Route Group Member section, highlight **Trunk_Rendezvous_to_Conductor_redundant** and click **Add to Route Group**.
6. Once both are added, they will appear in the **Current Route Group Members** section.

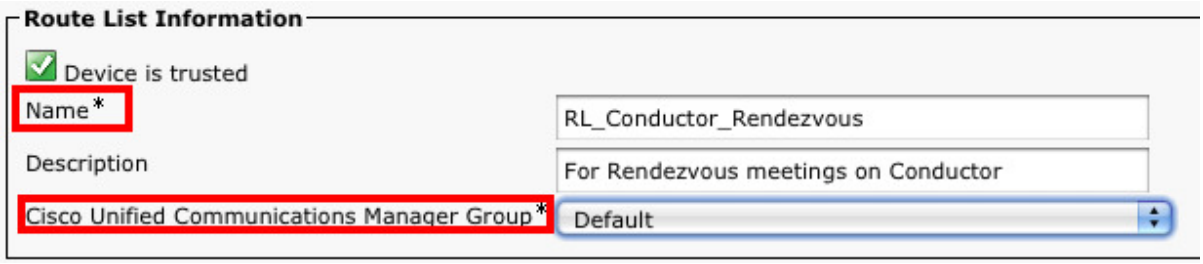
7. For load balancing rendezvous calls to the opposite TelePresence Conductor to the one used for ad hoc calls, ensure that Trunk_Rendezvous_to_Conductor_redundant is moved to the top of the list.
8. Click **Save**.

Task 11: Adding a route list for the route group

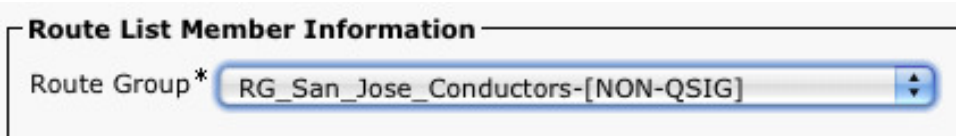
To configure a route list to use the route group that contains the SIP trunks to the TelePresence Conductor for rendezvous calls:

1. Go to **Call Routing > Route/Hunt > Route List**.
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:

Name	Enter a route list name
Cisco Unified Communications Manager Group	Select the appropriate group from the drop-down list



4. Click **Save**.
5. Click **Add Route Group**.
6. Next to the Route Group field select the route group created in Task 10: Adding a route group for the SIP trunks [p.18].



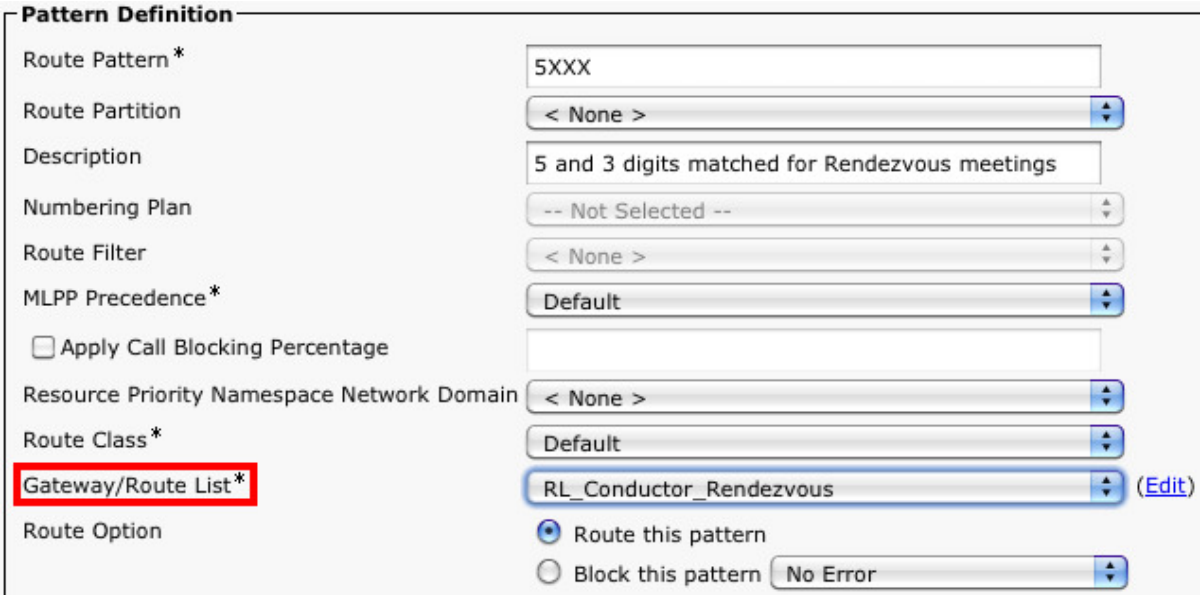
7. Click **Save**.
8. Click **Reset**.

Task 12: Editing the route pattern that matches the SIP trunk to TelePresence Conductorfor 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 **Find** and then select the relevant 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 route list used in Task 11: Adding a route list for the route group [p.19] from the drop-down list


Pattern Definition
Route Pattern*
5XXX
Route Partition
< None >
Description
5 and 3 digits matched for Rendezvous meetings
Numbering Plan
-- Not Selected --
Route Filter
< None >
MLPP Precedence*
Default
Apply Call Blocking Percentage
Resource Priority Namespace Network Domain
< None >
Route Class*
Default
Gateway/Route List*
RL_Conductor_Rendezvous
(Edit)
Route Option
Route this pattern
Block this pattern
No Error

4. Click **Save**.

Creating a system backup

To create a backup of TelePresence Conductor system data:

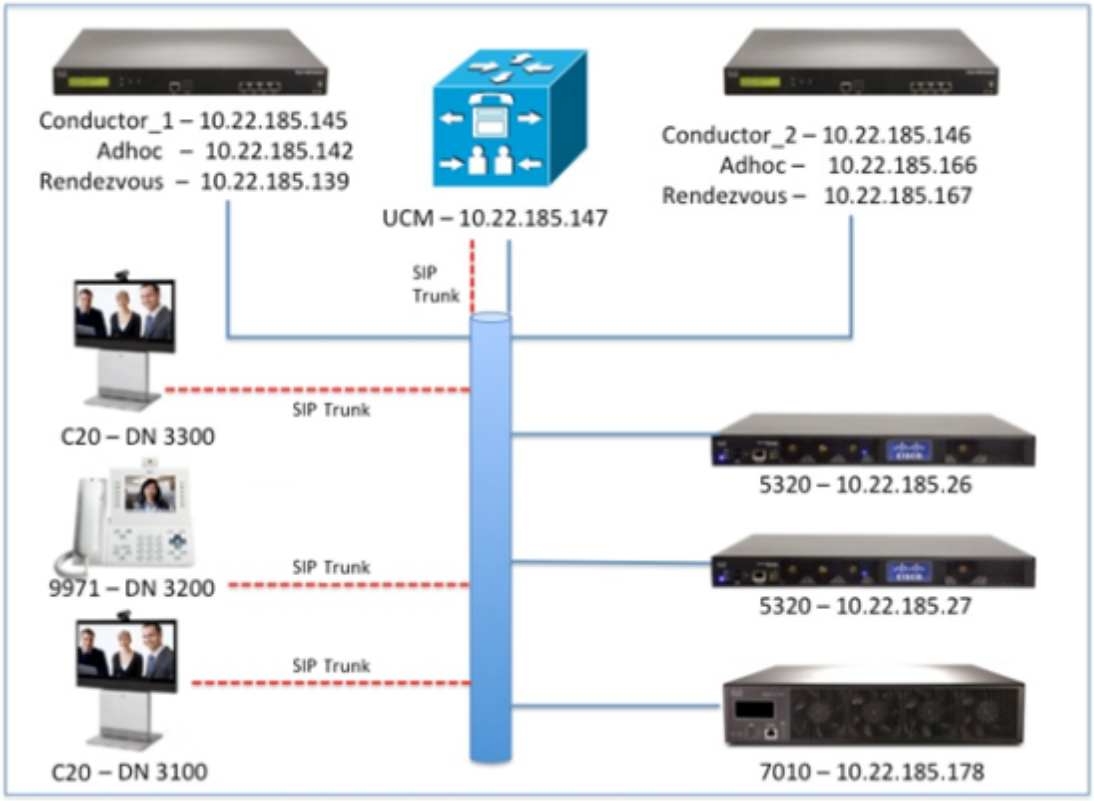
1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file.
   If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, 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.

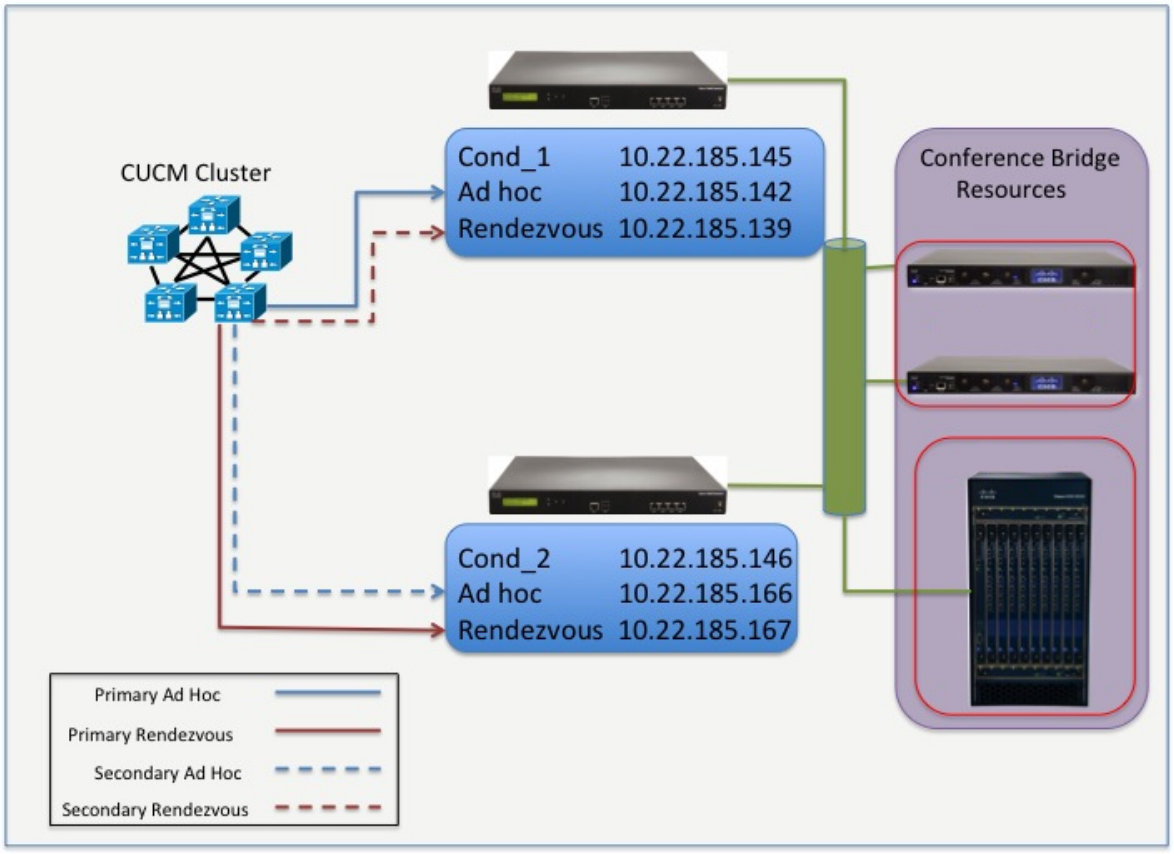
Log files are not included in the system backup file.

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

Testing system configuration

Once you have completed the configuration described in the previous sections, you should test that the system is working correctly as follows. The diagrams below are references for the testing steps:





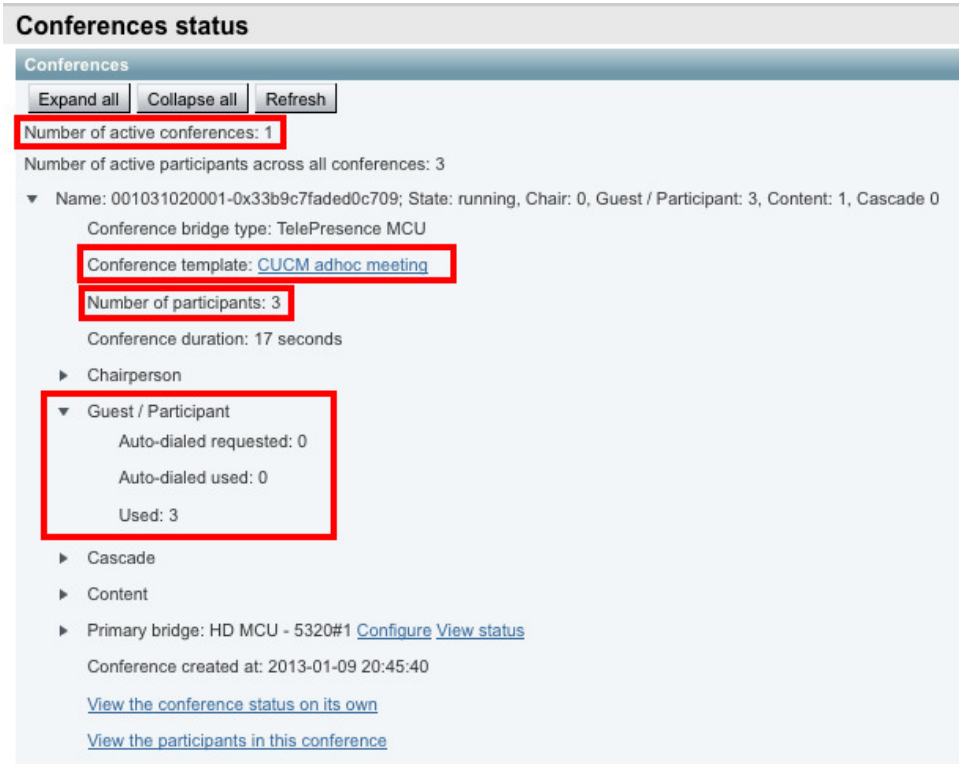
Creating an ad hoc conference

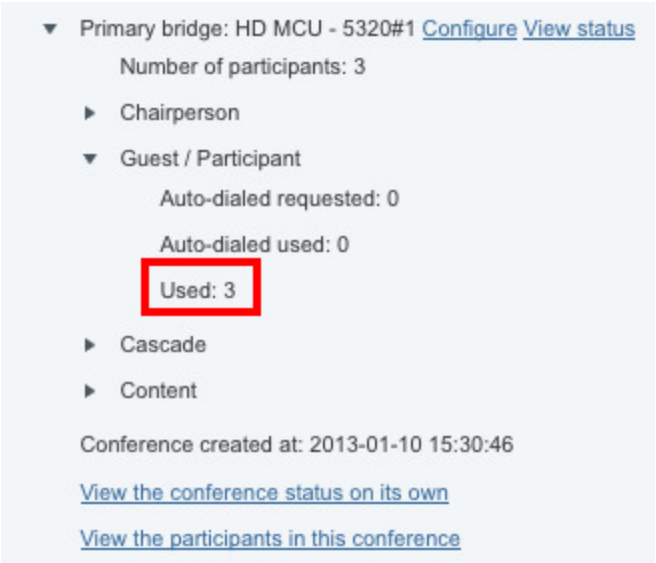
Perform the following test with both TelePresence Conductors operational, then with one switched on and the other off, then the first one off and second on.

To test that three Unified CM registered endpoints can join an ad hoc conference:

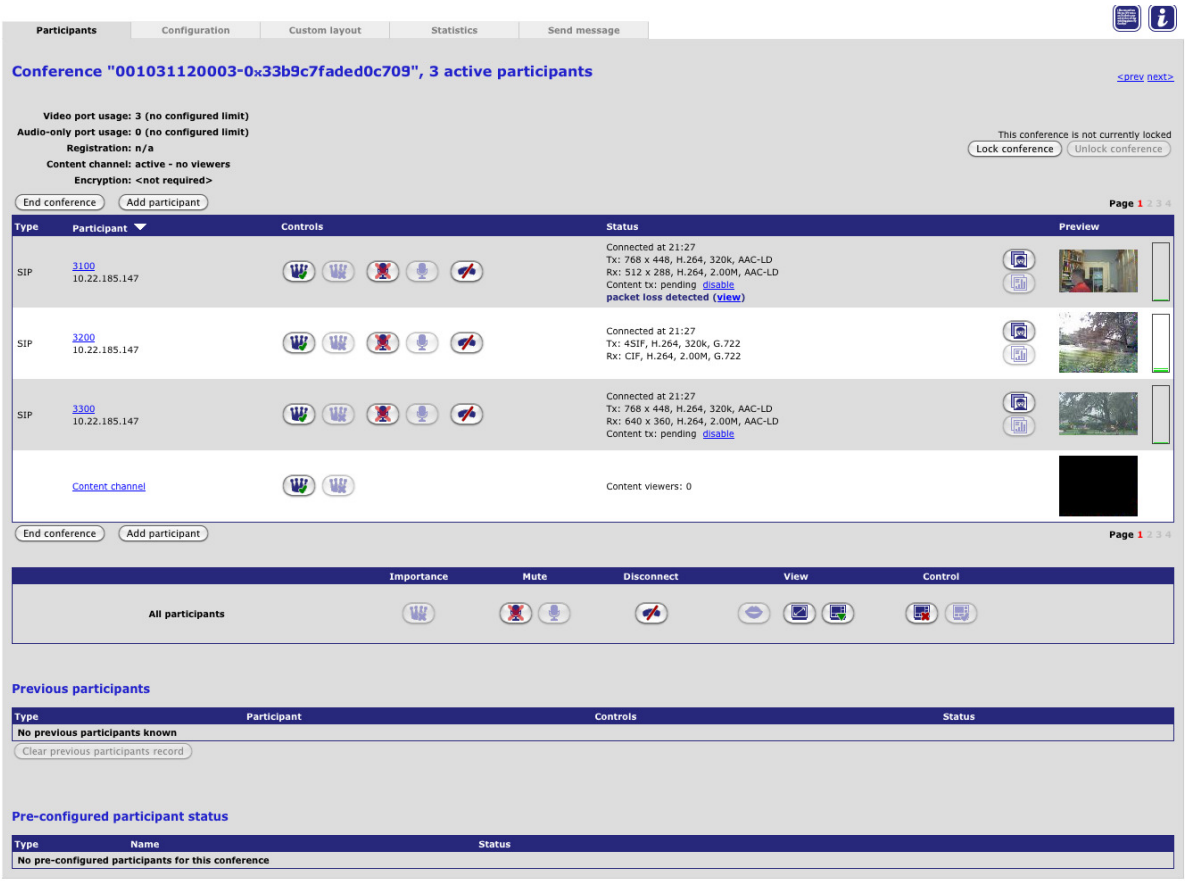
1. From the 9971 dial **3100**. Verify a video and audio session is established between the 9971 and the second C20.
2. From the 9971, press the conference button and dial **3300**. Verify a video and audio session is established between the 9971 and the second C20. Also note that the call between the 9971 and second C20 has been put on hold.
   Note: At this point the TelePresence Conductoris 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 MCU via **Cond_1**'s back-to-back user agent (B2BUA).

4. To verify the established call on the TelePresence Conductor, **Cond_1**, 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



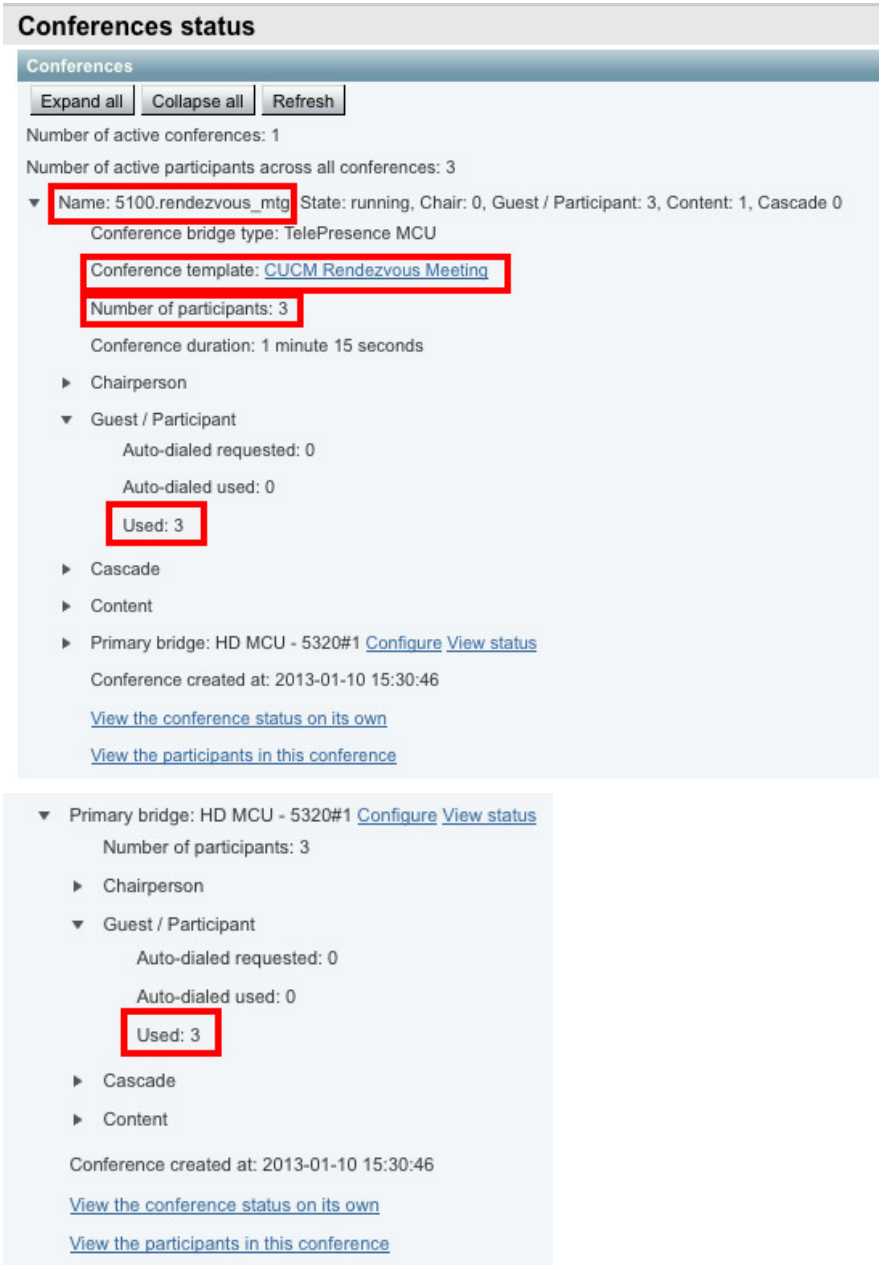
Creating a rendezvous conference

Perform the following test with both TelePresence Conductors operational, then with one switched on and the other off, then the first one off and second on.

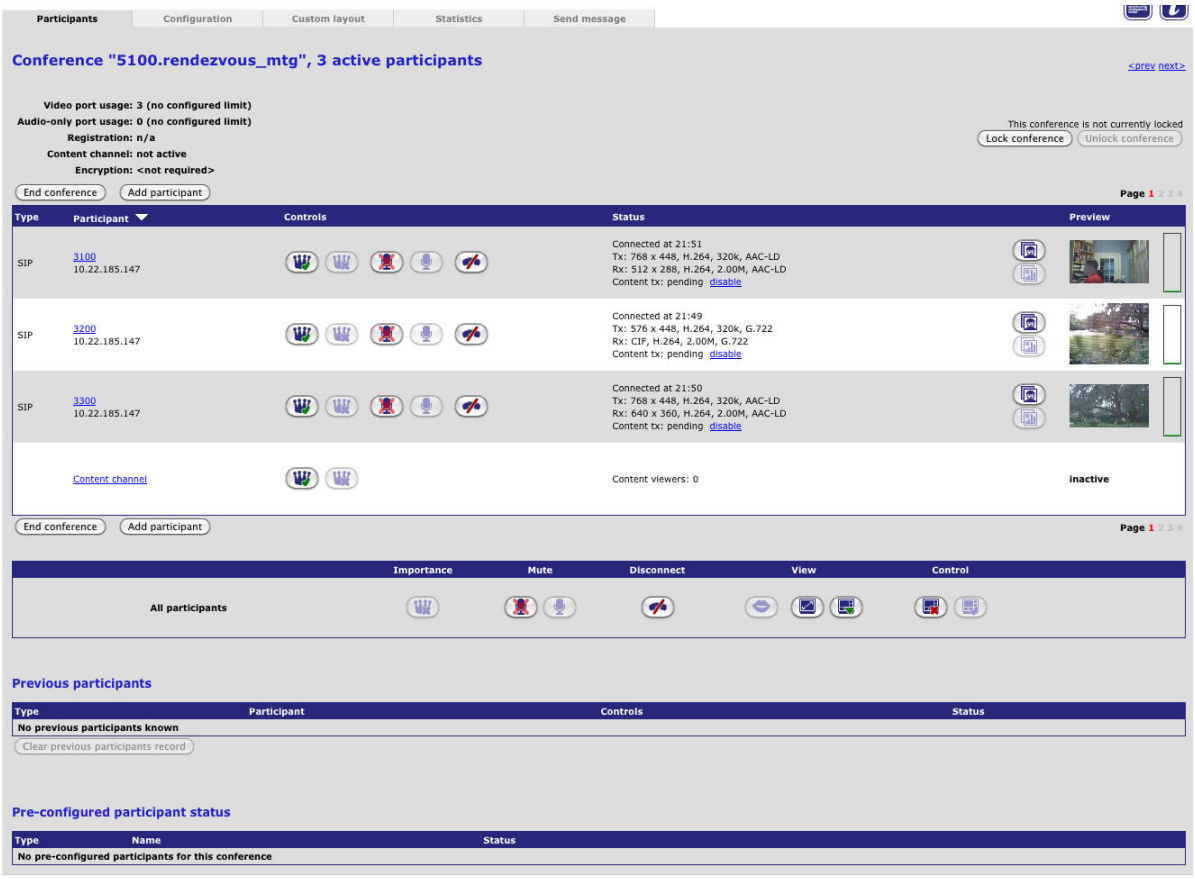
To test that two or more Unified CM registered endpoints can join a rendezvous conference:

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, **Cond_2**, that the call has been passed through the B2BUA, go to **Status > Conferences**.



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



Removing a TelePresence Conductor peer

To remove a TelePresence Conductor peer from a cluster, you must first remove the TelePresence Conductor from the Unified CM and then remove the TelePresence Conductor peer from the cluster.

Removing a TelePresence Conductor from Unified CM

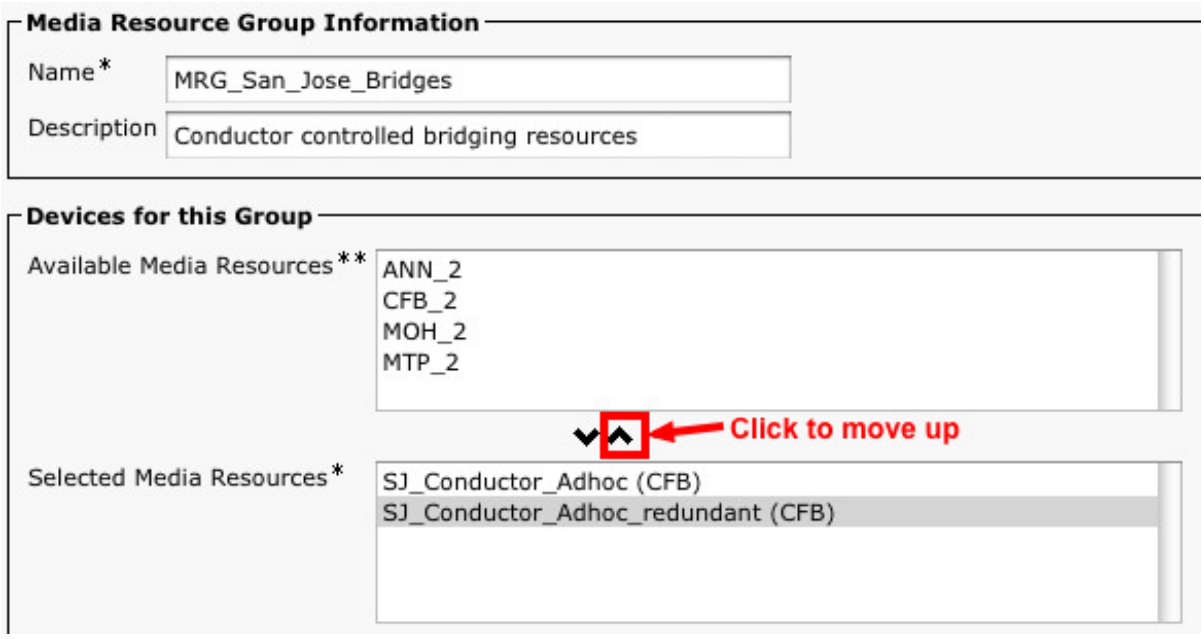
To remove a TelePresence Conductor from ad hoc calls you must remove the TelePresence Conductor from the Media Resource Group (MRG), and optionally delete the TelePresence Conductor from the Unified CM Conference bridges.

To remove a TelePresence Conductor from rendezvous calls you must remove the SIP trunk from the Unified CM to the TelePresence Conductor.

Removing the TelePresence Conductor from the Media Resource Group

(This step is only applicable for ad hoc conferences.)

1. Go to the Unified CM web interface and log in as an admin user.
2. Go to **Media Resources > Media Resource Groups**.
3. Click **Find** to list the Media Resource Groups.
4. Click on **MRG_San_Jose_Bridges**.
5. Highlight the TelePresence Conductor that you want to remove from the group and click on the ^ to move it to the *Available Media Resources* box.

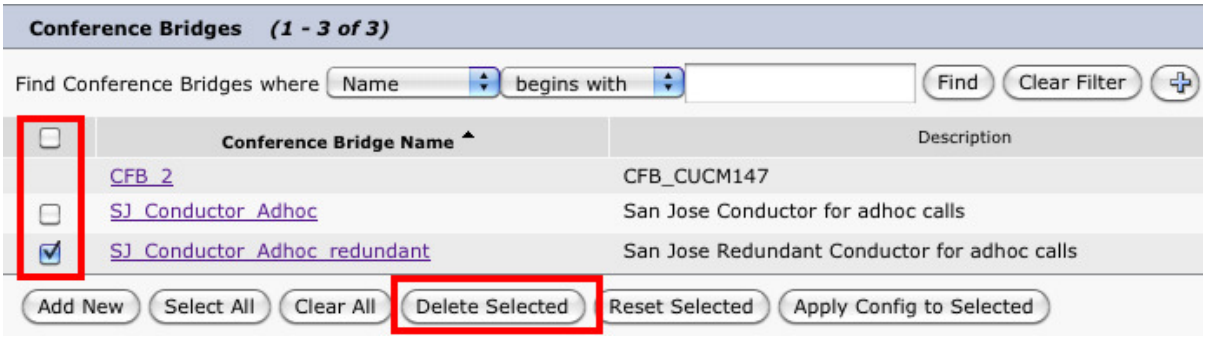


6. Click **Save**.

(Optional) Removing the TelePresence Conductor as a conference bridge

(This step is only applicable for ad hoc conferences.)

1. Go to the Unified CM web interface and log in as an admin user.
2. Go to **Media Resources > Media Resource Groups**.
3. Click **Find** to list the Conference Bridges.
4. Select the box next to the conference bridge and click **Delete Selected**.



Removing the SIP trunk to the TelePresence Conductor used for rendezvous conferences

(This step is only applicable for rendezvous conferences.)

1. Go to **Device > Trunk**.
2. Click **Find** to show the configured trunks.
3. Select the trunk that is used for the TelePresence Conductor being removed.
4. At the top of the page select the Cross (**Delete**).
5. Confirm the deletion by pressing **OK**.

Removing a peer from an existing cluster

Placing the peer in standalone mode

Before removing a live peer from a cluster, you must place the peer in standalone mode so that it no longer communicates with other peers in the cluster. If the peer is out of service and can no longer be accessed, you do not need to place it in standalone mode. However, you must still follow the instructions to remove it from the cluster in the next section: Updating all other peers in the cluster [p.31].

To place a peer into standalone mode:

1. Log in to the peer to be removed from the cluster as a user with administrator privileges.
2. Go to **System > Clustering**.
3. Delete the **Cluster pre-shared keyvalue**.
4. Delete all entries from the **Peer IP address** fields.
5. Click **Save**.
6. Go to **Maintenance > Restart options**.
7. Click **Restart**. When the TelePresence Conductor has restarted, it will be in standalone mode.
8. Optional: Delete the configuration or reconfigure the TelePresence Conductor.

Updating all other peers in the cluster

After the peer to be removed has been placed in standalone mode (or if the peer is out of service and cannot be contacted), you must update all other peers in the cluster so they no longer consider the removed peer to be part of their cluster.

To do this, on each remaining peer in the TelePresence Conductor cluster:

1. Go to **System > Clustering**.
2. From the relevant **Peer x IP address** field (x = 1, 2, or 3), delete the IP address of the peer that has been removed from the cluster.
3. Click **Save**.

Repeat these steps on each remaining peer.

Upgrading a cluster of TelePresence Conductors

The process described here is essentially disbanding, upgrading and then reclustering a cluster of TelePresence Conductors. In order to prevent downtime, one peer in the cluster is upgraded separately to the others, so that there is always at least one peer active and able to service conference requests from the Unified CMs until all peers have been upgraded and re-clustered.

Task 1: Removing a peer from the cluster

Follow the steps in Removing a TelePresence Conductor peer [p.29] to remove one peer from the TelePresence Conductor cluster.

Task 2: Upgrading the peer that has been removed from the cluster

On the TelePresence Conductor that has been removed from the cluster:

1. Go to the web interface and log in as a user with administrator privileges.
2. Go to **Maintenance > Upgrade**.
3. Click **Browse** and select the TelePresence Conductor software image.
4. Click **Upgrade**.
5. Follow the onscreen prompts.

Task 3: Configuring the upgraded peer to be a cluster of one peer

Follow the first two steps in Configuring the TelePresence Conductor [p.8] to create a new cluster of one peer with the upgraded TelePresence Conductor.

Task 4: Configuring Unified CM to use the upgraded peer

1. Follow the steps in Configuring Unified CM for ad hoc conferences [p.13] to add the upgraded TelePresence Conductor as a bridge to the Unified CM and to add it to an MRG and MRGL.
2. Follow the steps in Configuring Unified CM for rendezvous conferences [p.17] to remove the remaining TelePresence Conductors that have not yet been upgraded from Unified CM.

Task 5: Removing the other peers from the original cluster

Follow the steps in Removing a peer from an existing cluster [p.30] to remove the remaining TelePresence Conductors that have not yet been upgraded from the original cluster.

Task 6: Upgrading the other peers

Follow the steps in Task 2: Upgrading the peer that has been removed from the cluster [p.32] above to upgrade the remaining TelePresence Conductors.

Task 7: Adding the remaining peers into the new cluster

Follow the steps in Configuring the TelePresence Conductor [p.8] (sections 3 to the end) to create a new cluster of one peer with the upgraded TelePresence Conductor.

Task 8: Configuring Unified CM to use the upgraded peer(s)

1. Follow the steps in Configuring Unified CM for ad hoc conferences [p.13] to add the upgraded TelePresence Conductor as a bridge to the Unified CM and to add it to an MRG and MRGL.
2. Follow the steps in Configuring Unified CM for rendezvous conferences [p.17] to remove the remaining TelePresence Conductors that have not yet been upgraded from Unified CM.

Task 9: Testing the system with calls

Follow the steps in Testing system configuration [p.23] to make sure that the new cluster works properly with calls.

Troubleshooting

Unable to cluster the TelePresence Conductor

When running a TelePresence Conductor without a valid release key clustering is not supported. Contact your Cisco account representative to obtain release key and option keys.

Appendix 1: Unified CM version 8.6.2 configuration

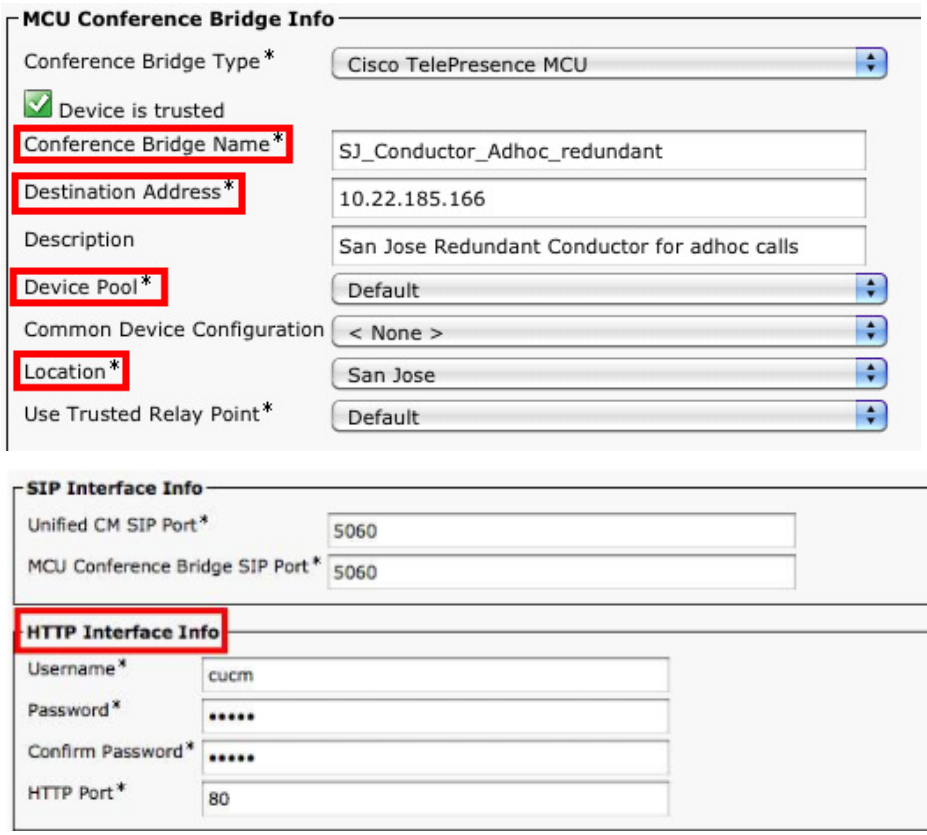
This section covers the differences between version 8.6.2 and version 9.0 or later of Unified CM when configuring it for use with the TelePresence Conductor. The individual steps in the section Creating a TelePresence Conductor cluster [p.7] are from a version 9.0 Unified CM and should be replaced with the relevant steps from this appendix for version 8.6.2 Unified CMconfiguration.

Add the secondary TelePresence Conductor as a bridge to the Unified CM for ad hoc conferences

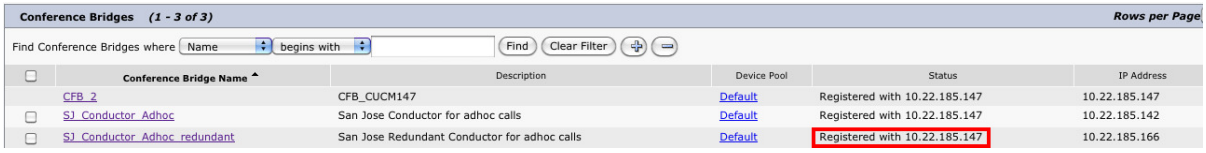
For Unified CM version 8.6.2, replace Task 7: Adding the secondary TelePresence Conductor as a bridge to the Unified CM for ad hoc conferences [p.13] with the following:

1. Go to **Media Resources > Conference Bridges**.
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 TelePresence MCU
Conference Bridge Name	Enter the TelePresence Conductor's Name
Destination Address	Enter the TelePresence Conductor's IP address
Device Pool	Select the appropriate pool
Location	Select the appropriate location
Username	Enter the username of the TelePresence Conductor administration user. 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'



4. Click **Save**.
5. Click **Reset** for the changes to take effect.
6. At the top right corner of the screen in the **Related Links:** field, select *Back to Find/List* and click **Go**. You will be taken back to the to the **Conference Bridges** page.
7. Verify that the TelePresence Conductor is registered with Unified CM.



Appendix 2: IP ports and protocols

It is unusual to have any sort of firewall between cluster peers, but if there is, the IP protocols and ports that must be open between each and every TelePresence Conductor peer in the cluster are listed below.

For cluster communications between TelePresence Conductor peers:

- UDP port 500 (ISAKMP) is used for PKI (Public Key Infrastructure) key exchange
- Standard SIP and H.323 signaling ports are used for calls
- UDP port 1719 is used for bandwidth updates between TelePresence Conductor peers
- IP protocol 51 (IPSec AH) is used for database synchronization
- UDP ephemeral ports are used for cluster management

If you are using the TelePresence Conductor's built-in **Firewall rules** feature then you must ensure that it is not configured to drop or reject traffic sent to UDP ports 4369 – 4380.

IPSec communications

For IPSec between TelePresence Conductor cluster peers:

- AES256 is used for encryption, SHA256 (4096 bit key length) is used for authentication; peers are identified by their IP address and are authenticated using a pre-shared key
- Main mode is used during the IKE exchange
- diffie-hellman group ‘modp4096’ is used

Document revision history

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

Revision	Date	Description
D15000.05	December 2013	Updated IP ports and protocols section
D15000.04	October 2013	Updated the Prerequisites section with changes introduced in XC2.2.1
D15000.03	August 2013	Updated for release XC2.2
D15000.02	May 2013	Updated for release XC2.1
D15000.01	December 2012	Initial release