Cisco TelePresence Conductor

Administrator Guide

XC1.2

D14826.03

May 2012

Contents

Introduction to the Cisco TelePresence Conductor

About the Cisco TelePresence Conductor

The Cisco TelePresence Conductor simplifies multiparty video communications. It lies within a video communications network, working in conjunction with one or more Cisco TelePresence Video Communication Servers (VCSs) and one or more conference bridges. It allows the video network to be configured such that spontaneous conferences or rendezvous* (a personal conference with a unique conference ID) may be easily provisioned, initiated, accessed and managed.

*often referred to as “MeetMe” conferences.

Cisco TelePresence Conductor features

The Cisco TelePresence Conductor is the focal point in a TelePresence network and acts in a similar manner to the conductor of an orchestra. It knows all of the individual conferencing components that have been configured to be used with it and their capabilities intimately, and will control all of these individual elements to achieve the best possible performance. This will ensure intelligent conference placement and optimum resource utilization and provides powerful, comprehensive administrator control.

It is tightly integrated with the industry-leading Cisco TelePresence MCUs and the Cisco TelePresence Video Communication Servers (VCSs). It will work with all standards-compliant endpoints.

The Cisco TelePresence Conductor can be deployed in a triple-redundant cluster (with nodes that may be geographically distributed), providing true reliability – conferencing is always available. The resilient architecture ensures service availability even if individual conference bridges or TelePresence Conductors are taken out of service.

It provides a single interface for service provisioning, no matter how many conference bridges there are. As scale increases, more conference bridges may simply be added without increasing provisioning overhead.

It scales from desktop through to immersive meeting room and from small businesses to the largest enterprises.

Conference personalization is supported to allow a user to get a consistent experience that satisfies their personal preferences (layouts, PINs, encryption etc.) irrespective of the conference bridge on which a conference is hosted.

Telepresence conferencing is elevated to a new level by ensuring a reliable and faultless conference experience with all of the conferencing components working together in harmony.

About this guide

This guide explains how to administer the Cisco TelePresence Conductor. However, because you must also configure your VCSs and conference bridges in a specific way in order for them to work with the TelePresence Conductor we have included sections that give an overview of the configuration of these devices as well.

If you are new to the TelePresence Conductor, we recommend that as a minimum you read the following sections (in order):

1. Before you start
2. Configuring system settings
3. Managing conference bridges
4. About creating conferences

Before you start

Before you add the Cisco TelePresence Conductor to your network, you will need to design an appropriate dial plan, and configure other network products to work with the TelePresence Conductor.

The following sections provide information on each of the prerequisite tasks:

- Designing a dial plan
- Configuring a conference bridge for use with the TelePresence Conductor
- Configuring a VCS for use with the TelePresence Conductor
- Configuring endpoints for use with the TelePresence Conductor
- Using CUCM with the Cisco TelePresence Conductor
- Testing your network configuration

Designing a dial plan

About dial plans

A dial plan defines all the possible aliases and call routes within your video network. A well-designed dial plan is a key component of a successful video network and should allow users to place calls simply and intuitively while retaining the ability to scale the network as more users and services are added.

General considerations

Before you add the Cisco TelePresence Conductor to your network, you will need to review your dial plan to ensure it supports the following aspects:

Note: there must not be any conflict between any **Incoming alias** or **Conference name** (used when Creating and editing conference aliases), the Call Policy prefix, or Conference bridge dial plan prefixes, otherwise you may experience unpredictable behavior. For more information, see Avoiding dial plan conflicts.

Area	Description
Conference aliases	These are the aliases that users will dial to create or join a conference. For example, you may want all TelePresence Conductor meetings to be accessed by dialing a conference address with the prefix **meet.**, and all lectures to be accessed by dialing either the prefix **show.** or the prefix **watch.**, depending on whether the user is a chairperson or guest. You will need to ensure that your dial plan routes these prefixes appropriately. For more information, refer to Creating and editing conference aliases and Configuring search rules with the TelePresence Conductor policy service as the target.
Conference names	These are the names that each conference will be known by on the host conference bridge. Lectures must be configured so that chairpersons and guests will dial different aliases but end up in the same conference. For more information, refer to Conference name (must use regex replace string).

Area	Description
Call Policy prefix	This is used to allow or prevent specified users from creating conferences. The TelePresence Conductor adds this prefix to a conference alias and sends the request back to the VCS for checking against its own Call Policy. For more information, refer to Using Call Policy.
Conference bridge dial plan prefixes	These are used by the VCS to route calls to conference bridges in the TelePresence Conductor's pool. Each conference bridge must have a unique prefix. For more information, refer to Dial plan prefix and Configuring a VCS search rule for each conference bridge.
Recording device	You can use the auto-dialed participants feature of the TelePresence Conductor to automatically add a recording device to a conference. To take advantage of this feature, your dial plan will need to use particular aliases to route such calls to your recording device. For more information, refer to Example - automatically recording a conference.
Deployments with both H.323 and SIP endpoints	SIP endpoints can only make calls in the form of URIs - for example **`name@domain`**. If the caller does not specify a domain when placing the call, the SIP endpoint automatically appends its own domain to the number that is dialed. So if you dial **`meet.alice`** from a SIP endpoint, the search will be placed for **`meet.alice@domain`**. H.323 endpoints do not append a domain, so if you dial **`meet.alice`** from an H.323 endpoint the call will be placed to **`meet.alice`**. If you have a deployment that includes both SIP and H.323 endpoints, you must ensure that your conference aliases and dial plan are set up so that users can dial the conference aliases from either type of endpoint. Some ways you can achieve this are: ■ Create all conference aliases in the form of a URI (for example **`meet.alice@example.com`**). All users will then have to dial the full URI to create or join a conference. ■ Using regular expressions, create conference aliases that will match an incoming alias with or without a domain appended. See Matching an alias with or without a domain appended for an example. ■ Create all conference aliases in the form of a URI (e.g. **`meet.alice@example.com`**), and set up a transform on the VCS to append the domain to any alias that does not include one. All users will then have to dial just the name portion of the alias (e.g. **`meet.alice`**) to create or join a conference. For full instructions on creating transforms on the VCS, see *Cisco TelePresence Video Communication Server Administrator Guide*.

Area	Description
CUCM	Endpoints registered to CUCM can only dial addresses made up of numbers. They cannot dial addresses in the form of URIs, such as `name@example.com`. If your deployment includes any endpoints registered to CUCM, you must ensure that your conference aliases and dial plan are set up so that users can dial a number to access conference aliases. ■ If your deployment ONLY includes endpoints registered to CUCM, you can achieve this by creating conference aliases in a format that uses numbers only. ■ If your deployment includes endpoints registered to CUCM as well as other endpoints that are capable of dialing URIs (in particular SIP endpoints, which can only dial URIs), then you must ensure that conference aliases can be accessed from an endpoint by dialing either a number or URI. Some ways you can achieve this are: • Create all conference aliases in the form of a URI, and set up transforms on the VCS that convert numbers into URIs • Create all conference aliases in the form of a number, and set up transforms on the VCS (or use ENUM, Findme or External Policy Server) to convert URIs into numbers. For full instructions on creating transforms on the VCS, see *Cisco TelePresence Video Communication Server Administrator Guide*. For full instructions on configuring a VCS and CUCM, see *Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide*.

Avoiding dial plan conflicts

The VCS is responsible for routing calls to the appropriate destination (for example, TelePresence Conductor, Cisco MCU, another VCS), or endpoint. It does this by means of search rules, which map search requests to target destinations based on factors such as the alias being dialed and the source of the request.

When creating your search rules on the VCS, you must ensure that they are specific enough so that:

- all conference aliases will route to the TelePresence Conductor only
- all calls beginning with any conference bridge dial plan prefix will route to the specified conference bridge only
- all calls beginning with the TelePresence Conductor's call policy prefix route to the TelePresence Conductor only, and no conference aliases begin with the same prefix.

Also make sure that no endpoints can register with a conference alias, conference bridge dial plan prefix or TelePresence Conductor call policy prefix; you can do this using registration allow or deny lists.

For further information about configuring search rules on the VCS, see *Cisco TelePresence Video Communication Server Administrator Guide*.

Configuring a conference bridge for use with the TelePresence Conductor

This section provides an overview of the configuration required on the conference bridge in order for it to work with the TelePresence Conductor and its VCS.

This release of the TelePresence Conductor supports *Cisco TelePresence MCUs* only. Future versions may support other types of conference bridges.

For information about configuring and using a Cisco TelePresence MCU, see *Cisco TelePresence MCU Online Help*.

Prerequisites

Before adding the conference bridges to the TelePresence Conductor's conference bridge pool, ensure that:

- they are running software version 4.2 or later (MCU 5310/5320 series must be running version 4.3(2.17))
- **if there is one or more Cisco MCU 5310/5320 used by the same** TelePresence Conductor**:** all other Cisco MCUs need to run software version 4.3(2.18) or later
- **if there is no MCU 5310/5320 used by the same** TelePresence Conductor**:** all Cisco MCUs are running the same software version
- they are reserved for the TelePresence Conductor's exclusive use and are not used by any other system, for example Codian Conference Director
- they have the specific configuration described below
- they are configured identically for all other settings not described below. These additional settings will depend on your network requirements, but failure to configure each conference bridge identically will result in unpredictable behavior or a potentially inconsistent user experience.

Note: do not use the Conference control menu on the Cisco TelePresence MCU in conjunction with the TelePresence Conductor, because some features do not consult the TelePresence Conductor before making changes to a conference, resulting in unpredicted behavior.

Cisco TelePresence MCU configuration

Page	Option	Information
Settings > Conferences	**Media port reservation**	Select *Disabled*.
	Failed preconfigured participants redial behavior	Select the option most appropriate for your deployment. See What if an auto-dialed participant can't be reached? for more information.
Settings > H.323	**H.323 gatekeeper usage**	Select *Enabled*.
	H.323 gatekeeper address	■ If you are using a single VCS, enter its IP address or host name. ■ If you are using a VCS cluster, enter the IP address or host name of one of the cluster's peers.
	Gatekeeper registration type	Select *MCU (standard)*.
	Prefix for MCU registrations	Ensure that this field is empty.
	MCU service prefix	Ensure that this field is empty.
	Allow numeric ID registration for conferences	Ensure that this option is **not** selected.
	Send resource availability indications	Ensure that this option is **not** selected.
Settings > SIP	**SIP registrar usage**	Select *Enabled*.
	SIP registrar domain	Enter the VCS's IP address or host name, or SIP domain.
	SIP registrar type	Select *Standard SIP*.
	Username	Enter the SIP URI or consult *Cisco TelePresence MCU Online Help* for further methods of configuring SIP.
	Allow numeric ID registration for conferences	Ensure that this option is **not** selected.
	SIP proxy address	Enter the IP address or host name of a SIP proxy used by the VCS or one peer of the VCS cluster.
	Outgoing transport	Select *TLS* or if this is not available, select *TCP*. Ensure that the SIP transport protocol matches the protocol selected for the neighbor zone on the VCS.

Page	Option	Information
Network > Services	**SIP (TCP)**	If you have selected an **Outgoing transport** of *TCP*: ■ ensure that this option is selected ■ ensure that the port listed here is the same as the port listed on the VCS for the SIP connection to this zone (**VCS configuration > Zones**, click on the zone name and scroll down to the **SIP** section).
	Encrypted SIP (TLS)	If you have selected an **Outgoing transport** of *TLS*: ■ ensure that this option is selected ■ ensure that the port listed here is the same as the port listed on the VCS for the SIP connection to this zone (**VCS configuration > Zones**, click on the zone name and scroll down to the **SIP** section) ■ ensure that the certificate on the MCU is valid, if **TLS Verification** is enabled on the VCS.
	Incoming H.323	■ Ensure that this option is selected. ■ Ensure that the port listed here is the same as the port listed on the VCS for the H.323 connection to this zone (**VCS configuration > Zones**, click on the zone name and scroll down to the **H.323** section).
Conferences > Templates (then select the template)	**When only guests remain**	Ensure that this option is set to *Take no action*.

Page	Option	Information
Users > Add new user	Use this page to create a new account for the TelePresence Conductor to use when logging in to this MCU. (The TelePresence Conductor must log in to the MCU in order to manage conferences and retrieve MCU resource information.) Later, when you add this MCU to the TelePresence Conductor's conference bridge pool you will need to provide the **User ID** and **Password** that have been set up here. **Note:** we strongly recommend that you set up a new account; do not use the MCU's default admin account.	
	User ID	We recommend you use a name that makes it clear that this account is used by the TelePresence Conductor. While it is possible to use the same User ID for the TelePresence Conductor on all MCUs in the pool, for security reasons we recommend you use a different User ID on each MCU.
	Password	This must not be blank. For security reasons we recommend you use a strong password.
	Disable user account	Ensure that this option is **not** selected.
	Lock password	Select this option.
	Force user to change password on next login	Ensure that this option is **not** selected.
	Privilege level	Select *administrator*.
Gatekeeper > Built-in gatekeeper	**Status**	Select *Disabled*.

The rest of the MCU settings will depend on your network configuration.

Configuring a VCS for use with the TelePresence Conductor

This section provides an overview of the configuration required on a Cisco TelePresence Video Communication Server (VCS) in order for it to work with the TelePresence Conductor and its pool of conference bridges. It assumes a working knowledge of the VCS. For further information about configuring and using the VCS, see *Cisco TelePresence Video Communication Server Administrator Guide*.

Supported VCS versions

Cisco TelePresence Conductor version XC1.1 and later supports Cisco TelePresence Video Communication Server version X6.0 and later.

Prerequisites

- Before you start configuring the VCS, you must have designed a dial plan that includes the conference aliases to be supported by the VCS and the search rule prefixes that will allow the VCS to route calls directly to the VCS's conference bridge pool. See Designing a dial plan for more information.

- Ensure that the VCS has been configured appropriately for your network and has appropriate licenses installed, including sufficient call licenses.

Adding the TelePresence Conductor as a policy service

On the VCS, go to the **Policy services** page (**VCS configuration > Dial plan > Policy services**) and create a new policy service for the TelePresence Conductor as follows:

Field	Input
Name	Enter a name for the service, e.g. **`Conductor`**.
Description	In this optional field you can enter a description of the service. This will appear as a tooltip when you hover your mouse pointer over this policy service in the list.
Protocol	Select *HTTPS*
Certificate verification mode	If you are using the default certificate - or a certificate signed by a CA not in the Trusted CA certificate of the VCS - then you must select *Off*. If you have followed best practice and uploaded a non-default Server certificate to your TelePresence Conductor (and updated the Trusted CA certificate on your VCS if required) then we strongly recommend that you should select *On*.
HTTPS certificate revocation list (CRL) checking	If you have configured your VCS appropriately and followed the procedures defined in the *VCS documentation* to enable HTTPS certificate revocation list (CRL) checking, select *On*. Otherwise select *Off*.
Server 1-3 address	If you are connecting to a single TelePresence Conductor, enter its IP address or FQDN in the **Server 1 address** field. If you have a cluster of TelePresence Conductors, enter the IP address or FQDN of each peer in one of the three **Server address** fields. The order in which the addresses are added is not important.
Path	Enter **`api/conference_controller/conference/conference_factory.cpl`**
Status path (VCS version X6.1 and later)	Use the default of **`status`**
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.
Default CPL	You can leave this as the default but to aid in troubleshooting we recommend you change it to: **`<reject status='504' reason='TelePresence Conductor policy service unavailable'/>`**

Please be aware that

- it is possible to add five different policy services per VCS (or VCS cluster) to support deployments where more than one TelePresence Conductor (or TelePresence Conductor cluster) is required. Care must be

taken to ensure that there is no dial plan overlap between the different policy services. If you are in doubt, talk to your Cisco technical representative.

- there is a theoretical risk from Man-in-the-middle attacks unless you deploy valid certificates on your video network infrastructure equipment and enable certificate verification.
- Cisco strongly recommends that you generate custom certificates for your video network infrastructure devices. This can be achieved by purchasing them from a reputable commercial certificate authority or by running your own Certificate Authority. If running your own Certificate Authority ensure all trusted CA certificates are updated on the relevant devices along with the custom server certificate.
- if your certificate gets stolen (e.g. due to a server room break-in), then the risk from Man-in-the-middle attacks arises again. Enabling CRL checking on the VCS could help you should such a theft occur, as you could get your CA to revoke the stolen certificate.

Configuring search rules with the TelePresence Conductor policy service as the target

On the VCS, go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**). For every conference alias that is or will be configured on the TelePresence Conductor, ensure that there is a search rule that matches that alias and has the TelePresence Conductor policy service as its target. The search should be set to *Stop* on a successful match.

Note: you do not need to configure a separate search rule for each conference alias if you use pattern matching and regular expressions when creating your search rules.

Example - prefix matching

If all your conference aliases for meetings begin with **meet.** then you could use prefix matching to create a single search rule for all meetings as follows:

Field	Example input
Rule name	Enter `Conductor meeting`
Mode	Select *Alias pattern match*
Pattern type	Select *Prefix*
Pattern string	Enter `meet.`
Pattern behavior	Select *Leave*
On successful match	Select *Stop*
Target	Select the name you gave the policy service, e.g. *Conductor*, from the drop-down list.
State	Select *Enabled*

The rest of the settings should be configured according to your dial plan and network settings.

Example - regular expression

If all your conference aliases begin with one of three prefixes:

- **meet.** for participants dialing in to a meeting
- **show.** for chairpersons dialing in to a lecture

- **watch.** for guests dialing in to a lecture

then you could use a regular expression to create a single search rule for all conferences as follows:

Field	Example input
Rule name	Enter `Conductor conference`
Mode	Select *Alias pattern match*
Pattern type	Select *Regex*
Pattern string	Enter `meet\..+|show\..+|watch\..+`
Pattern behavior	Select *Leave*
On successful match	Select *Stop*
Target	Select the name you gave the policy service, e.g. *Conductor*, from the drop-down list
State	Select *Enabled*

The rest of the settings should be configured according to your dial plan and network settings.

Adding each conference bridge as a neighbor zone

On the VCS, go to the **Zones** page (**VCS configuration > Zones**). For every conference bridge in the TelePresence Conductor's conference bridge pool, create a Neighbor zone with the following settings:

Field	Input
Name	Enter a name for the zone, e.g. `Conductor MCU 1` For ease of reference, we recommend that you use the same name for the conference bridge both here on the VCS (when configuring the conference bridge zone) and on the TelePresence Conductor (when adding the conference bridge to the pool).
Type	Select *Neighbor*
H.323 Mode	Select *On*
SIP Mode	Select *On*
SIP transport	Select *TLS* if your conference bridge has the encryption option key, otherwise select *TCP*. Ensure that the SIP transport protocol matches the protocol selected for SIP registration on the conference bridge.
Peer 1 address	Enter the IP address or FQDN of the conference bridge
Zone profile	■ For VCS versions 7.0 and later, select *Infrastructure device* ■ For earlier VCS versions select *Non-registering device*

The rest of the zone configuration options will depend on your network configuration.

Configuring a VCS search rule for each conference bridge

On the VCS, go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**). For every conference bridge in the TelePresence Conductor's conference bridge pool, create a separate search rule based on the **Dial plan prefix** that was assigned to that conference bridge when it was added to the pool. This rule should match the prefix but remove it before forwarding the call to the conference bridge. The search should be set to *Stop* on a successful match.

Note: each conference bridge must have a unique **dial plan prefix**.

See Adding and editing conference bridges for more information about configuring the conference bridge dial plan prefix.

Example

For example, if a conference bridge has been configured with a **dial plan prefix** of **555** on the TelePresence Conductor you could set up a search rule on the VCS as follows:

Field	Example input
Mode	Select *Alias pattern match*
Pattern type	Select *Prefix*
Pattern string	Enter `555`
Pattern behavior	Select *Strip*
On successful match	Select *Stop*
Target	Select the name you gave the conference bridge zone, e.g. *Conductor MCU 1*, from the drop-down list
State	Select *Enabled*

The rest of the fields should be configured according to your dial plan and network settings.

Using TelePresence Conductor and Multiway™

The VCS supports Multiway, a conferencing feature that enables video endpoint users to introduce a third party into an existing call. The deployment of Multiway with the TelePresence Conductor requires version 6.0 or later of the VCS and version 4.2 or later of the Cisco MCU. It is possible to use both the TelePresence Conductor and Multiway within the same deployment, as long as you ensure that:

- **either** any conference bridges that are part of the TelePresence Conductor's conference bridge pool are not simultaneously used for Multiway
- **or** the Multiway template is incorporated into the dial plan in such a way that the aliases generated by it are sent to TelePresence Conductor
- you refrain from adding auto-dialed participants that are or could be using Multiway (for more information see Using auto-dialed participants and Multiway)

For more information on how to use TelePresence Conductor and Multiway, see *Multiway Cisco TelePresence Deployment Guide*.

Configuring endpoints for use with the TelePresence Conductor

No special endpoint configuration is required to enable endpoint users to dial conference aliases (the method by which they can create or join conferences using the TelePresence Conductor). As long as an endpoint can successfully register with the Cisco TelePresence Video Communication Server (VCS), it can make use of the TelePresence Conductor (assuming of course that you have an appropriate dial plan in place).

However, you should bear in mind that dialing behavior differs between SIP and H.323 endpoints. If you have a deployment that includes both types of endpoint, you must ensure your conference aliases and dial plan are set up to support this. Refer to Deployments with both H.323 and SIP endpoints for more information.

Using CUCM with the TelePresence Conductor

The TelePresence Conductor includes native support for CUCM 8.6(2) and later via the VCS. As long as there is an appropriately configured SIP trunk between CUCM and VCS, any endpoints registered with CUCM will be able to create and join conferences on the TelePresence Conductor.

For full instructions on configuring a VCS and CUCM, see *Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide*.

For further information on designing a dial plan that includes endpoints registered to CUCM, see CUCM.

Testing your network configuration

After you have configured your conference bridges, configured your VCS, and configured your endpoints you should test that all these systems are working together properly before you add the TelePresence Conductor to your network.

To do this, create a test conference on the Cisco MCU in the same way that the TelePresence Conductor would create it once it is part of the setup. Ensure that you can dial directly into it as both a chairperson and guest from endpoints registered to the VCS. Follow these steps:

1. Log in to the Cisco MCU.
2. From **Conferences > Conference list**, select **Add new conference**. This allows you to create the test conference. Enter a Name, Numeric ID and Guest numeric ID for the test conference, for example:
   - **Name:** `Test`
   - **Numeric ID:** `123`
   - **Guest numeric ID:** `456`

   and click **Add conference**.
3. To test that an endpoint user can dial into the test conference as a chairperson, from an endpoint registered to the VCS, dial the **Dial plan prefix** for which a search rule has been defined on the VCS (in this case `555`), followed by the **Numeric ID**. In this example you would dial `555123`. You should be taken to the test conference on the Cisco MCU.
4. To test that another endpoint user can dial into the test conference as a guest, from a second endpoint dial the **Dial plan prefix** for which a search rule has been defined on the VCS (in this case `555`), followed by the **Guest numeric ID**. In this example you would dial `555456`. You should be taken to the same conference on the Cisco MCU.

5. To delete the conference created above, select the conference from the list under **Conferences > Conference list > [x] scheduled conferences** and select **Delete selected.**

If you are unable to perform the test successfully, do not attempt to add the TelePresence Conductor to your network until the issues have been identified and resolved.

Using the web interface

Configuration of the TelePresence Conductor is normally carried out through the web interface. This section covers the following topics:

Logging in to the web interface

To use the web interface, you must log in as follows:

1. Open a browser window and in the address bar type either:
   - the IP address of the system (this is `192.168.0.100` by default and should be changed during the commissioning process)
   - the FQDN of the system.

   The **Administrator login** page appears.
2. Enter a valid administrator **Username** and **Password** (see the Administrator account section for details on setting up administrator accounts) and click **Login**.

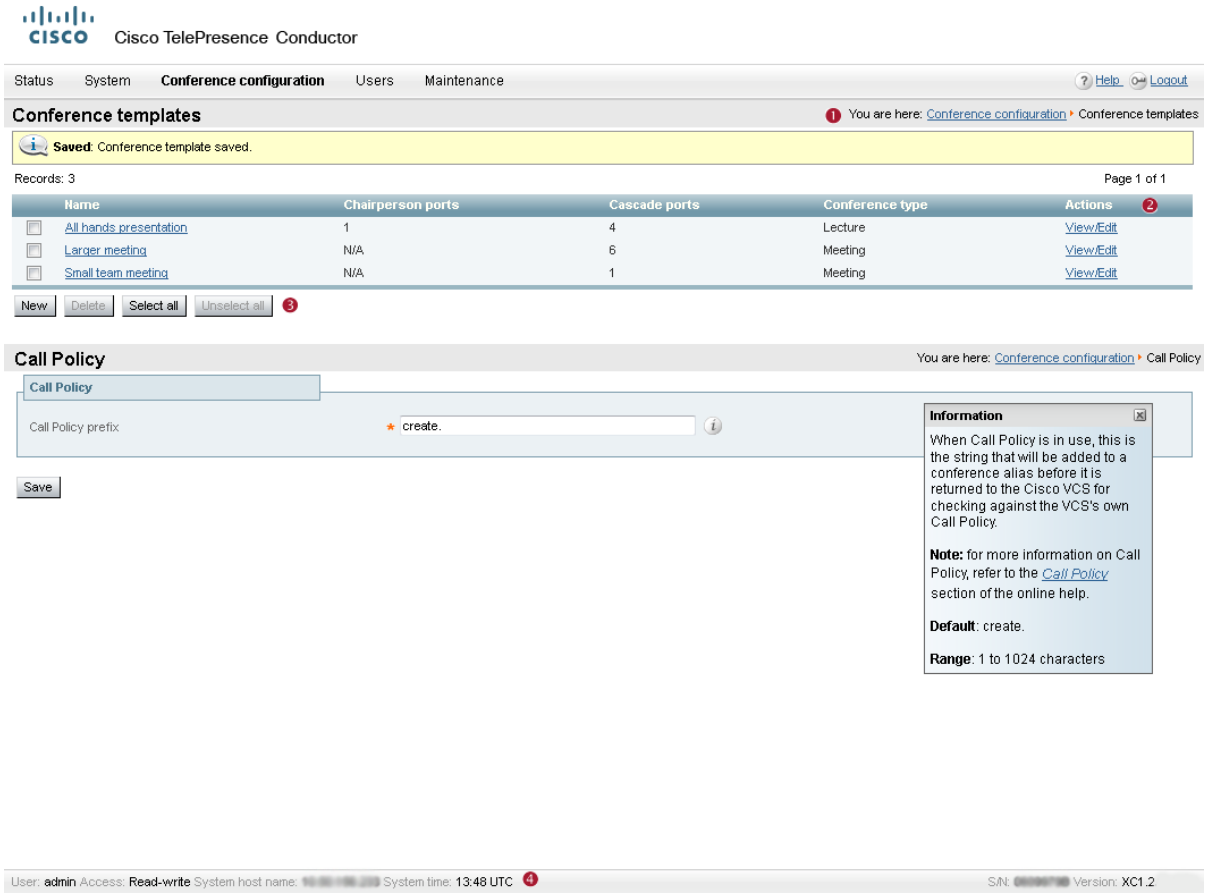
You are presented with the **Overview** page.

Note: the default password for the administrator user is **TANDBERG**. The TelePresence Conductor's conference functionality will be disabled until this password has been changed. It is important to select a secure password for the administrator user.

Note: when logging in to the TelePresence Conductor web interface, you may receive a warning message regarding the TelePresence Conductor's security certificate. To avoid this, ensure that you replace the factory default certificate with your own valid certificate.

Web page features and layout

This section describes the features that can be found on some or all of the web interface pages.



The elements included in the example web pages shown above are described in the table below.

Page element		Description
Page name and location		Every page shows the page name and the menu path to that page. Each part of the menu path is a link; clicking on any of the higher level menu items takes you to that page.
System alarm		This icon appears on the top right corner of every page when there is a system alarm in place. Click on this icon to go to the Alarms page which gives information about the issue and its suggested resolution. There should never be any active alarms on a fully functional, correctly configured system.
Help		This icon appears on the top right corner of every page. Clicking on this icon opens a new browser window with help specific to the page you are viewing. It gives an overview of the purpose of the page, and introduces any concepts configured from the page.
Log out		This icon appears on the top right corner of every page. Clicking on this icon ends your administrator session.
Field level information		An information box appears on the configuration pages whenever you either click on the information icon or click inside a field. This box gives you information about the particular field, including where applicable the valid ranges and default value. To close the information box, click on the X at its top right corner.

Page element		Description
Information bar		The TelePresence Conductor provides you with feedback in certain situations, for example when settings have been saved or when you need to take further action. This feedback is given in a yellow or red information bar at the top of the page.
Sorting columns	2	Click on column headings to sort the information in ascending and descending order.
Select All and Unselect All	3	Use these buttons to select and unselect all items in the list.
Mandatory field	*	Indicates an input field that must be completed.
System Information	4	The name of the user currently logged in and their access privileges, the system name (or LAN 1 IPv4 address if no system name is configured), local system time, hardware serial number and TelePresence Conductor software version are shown at the bottom of the page.

How page navigation is shown in this guide

Instructions for navigating the web interface are shown in the format **Menu option 1 > Menu option 2** followed by the **Name** of the page that you are taken to in order to perform a task.

Supported browsers and characters

Supported browsers

The TelePresence Conductor web interface is designed for use with Internet Explorer 8 or 9, Firefox 3 or higher, or Chrome. Later versions of these browsers may also work, but are not officially supported. It may work with Opera and Safari, but you could encounter unexpected behavior.

JavaScript and cookies must be enabled to use the TelePresence Conductor web interface.

Supported characters

The TelePresence Conductor supports the following characters when entering text in the web interface:

- the letters A-Z and a-z
- decimal digits (0-9)
- underscore (_)
- minus sign / hyphen (-)
- equals sign (=)
- plus sign (+)
- at sign (@)
- comma (,)
- period/full stop (.)

- exclamation mark (!)
- spaces

The following characters are allowed but we recommend that you do not use them:

- tabs
- angle brackets (< and >)
- ampersand (&)

Case sensitivity

Most text items entered through the web interface are case-insensitive. The exceptions are passwords.

Using the basic conference configuration wizard

The TelePresence Conductor has a basic conference configuration wizard, which takes you through the steps required to configure the initial conference configuration for a meeting-type conference.

To access the wizard go to the **Basic conference configuration wizard** page (**Conference configuration > Basic conference configuration wizard**).

Before starting the wizard, ensure you have:

- changed your root and admin passwords
- assigned an IP address, which you can use to access the TelePresence Conductor user interface
- set the correct NTP settings
- configured your conference bridge according to the instructions in the section Configuring a conference bridge for use with the TelePresence Conductor
- configured your VCS according to the instructions in the section Configuring a VCS for use with the TelePresence Conductor

And ensure you have the following information at hand:

- Conference bridge IP address or FQDN
- Protocol used to communicate with the conference bridge (HTTP or HTTPS) - We recommend using HTTPS
- Conference bridge username and password
- Dial plan prefix configured on the VCS

Configuring system settings

The **System** menu allows you to set up the following items:

- System administration
- Ethernet
- IP configuration
- DNS
- Time
- SNMP

System administration

Most TelePresence Conductor administration can be performed using the web interface. The **System administration** page (**System > Administration**) is used to configure additional administration options available to administrators.

The configurable options are:

Field	Description
TTY logins	Determines whether the system can be accessed locally via either the serial port (for a physical system) or VMware console (for a virtual machine). **Default:** On
SSH service	Determines whether the TelePresence Conductor can be accessed via SSH and SCP.
LCD panel	Determines whether any information will be displayed on the LCD panel on the front of the TelePresence Conductor unit. *On*: the LCD panel will display information such as Cisco TelePresence Conductor, the **Local host name** (if configured), the LAN 1 IPv4 address and any alarms that may apply to the unit. *Off*: The LCD panel will display "Cisco". **Default:** On
HTTP Strict Transport Security (HSTS)	Determines whether web browsers are instructed to only ever use a secure connection to access this server. Enabling this feature gives added protection against man-in-the-middle (MITM) attacks. *On:* the Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time. *Off:* the Strict-Transport-Security header is not sent, and browsers work as normal. **Note:** you must restart the system for any changes to take effect. **Default:** On

It is also possible to administer the TelePresence Conductor via a PC connected directly to the unit via a serial cable. This access is restricted to logging in as root.

Because access to the serial port allows the password to be reset, it is recommended that you install the TelePresence Conductor in a physically secure environment.

HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) provides a mechanism, where a web server forces a web browser to communicate with it using secure connections only.

As of January 2012, this mechanism is supported by the following browsers:

- Chrome, versions 4 and later
- Firefox, versions 4.0.211.0 and later

When HSTS is enabled, a browser that supports HSTS will:

- Automatically turn any insecure links to the website into secure links (for example, `http://example.com/page/` is modified to `https://example.com/page/` before accessing the server).
- Only allows access to the server if the connection is secure (for example, the server's TLS certificate is valid, trusted and not expired).

Browsers that do not support HSTS will ignore the Strict-Transport-Security header and work as before. They will still be able to access the server.

Note that compliant browsers only respect Strict-Transport-Security headers if they access the server through its fully qualified name (rather than its IP address).

TelePresence Conductor unit front panel

By default, during normal operation the front panel of the TelePresence Conductor unit shows Cisco TelePresence Conductor, the **Local host name** (if configured), the LAN 1 IPv4 address and any alarms that may apply to the unit.

Ethernet

The **Ethernet** page (**System > Ethernet**) is used to configure the speed of the connection between the TelePresence Conductor and the Ethernet switch to which it is connected. The speed and duplex setting must be set to the same value on both systems.

The default is *Auto*, which means that the two systems will auto-negotiate the appropriate speed and duplex setting.

Note: you are recommended to use the default value of **Auto** unless the switch to which you are connecting is unable to auto-negotiate. A mismatch in Ethernet speed settings between the TelePresence Conductor and Ethernet switch will result in packet loss and may make the system inaccessible.

Status

The **Status** section of the page displays the following information for the LAN 1 port:

Field	Description
MAC address	The MAC address of the TelePresence Conductor's Ethernet device for that LAN port.

Field	Description
Speed	The speed of the connection between the LAN port on the TelePresence Conductor and the Ethernet switch. If *Auto* has been selected, this will show the actual speed that has been negotiated.

IP configuration

The **IP** page (**System > IP**) is used to configure the IP settings of the TelePresence Conductor.

Network configuration

In this section of the web page you can set the default **IPv4 gateway** used by the TelePresence Conductor. This is the gateway to which IP requests are sent for IP addresses that do not fall within the TelePresence Conductor's local subnet. The default **IPv4 gateway** is `127.0.0.1`, which should be changed during the commissioning process.

LAN 1

LAN 1 is the primary network port on the TelePresence Conductor.

In this section of the web page you can configure the **IPv4 address** and **subnet mask** for this port. Their default values are `192.168.0.100` and `255.255.255.0` respectively. The **IPv4 address** should be changed during the commissioning process. The **subnet mask** should be changed if necessary.

DNS

The **DNS** page (**System > DNS**) is used to configure the TelePresence Conductor's DNS settings and DNS servers.

DNS settings

System host name

The **System host name** defines the DNS host name by which this TelePresence Conductor is known. Note that this is not the fully-qualified domain name, just the host label portion.

The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit.

The table below shows where the **System host name** is used, and what will be shown instead, if it is not configured.

Location	Notes
Web interface	If not configured, the system's IP address will be used instead.
Front panel of unit (so that you can identify it when it is in a rack with other systems)	If not configured, the system's IP address will be used instead. If the **System host name** is longer than 16 characters, only the last 16 characters are shown in the display on the front panel.

Location	Notes
Remote log server	If not configured, the remote syslog server will show a default name of **TANDBERG**.

Note: the **System host name** must be unique for each peer in a cluster.

You are recommended to give the TelePresence Conductor a **System host name** that allows you to easily and uniquely identify it.

Domain name

The **Domain name** is used when attempting to resolve unqualified server addresses (for example `ldapserver`). It is appended to the unqualified server address before the query is sent to the DNS server. If the server address is fully qualified (for example `ldapserver.mydomain.com`) or is in the form of an IP address, the domain name is not appended to the server address before querying the DNS server.

It applies to the following configuration settings in the TelePresence Conductor:

- LDAP server
- Configuring the NTP servers
- Remote logging server
- Conference bridges

You are recommended to use IP addresses for conference bridges, and an IP address or FQDN (Fully Qualified Domain Name) for all server addresses.

The **Domain name** may also be used along with the local **System host name** to identify references to this TelePresence Conductor in SIP messaging.

Note: the FQDN of the TelePresence Conductor is the **System host name** plus the **Domain name**.

DNS servers

You must specify at least one DNS server to be queried for address resolution if you want to use FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, or conference bridges).

Note: if you do not configure any DNS servers, you must ensure that your NTP servers are configured using IP addresses so that NTP time can still be obtained. This is because NTP time is required for correct system operation.

Default DNS servers

Note: for reliability we recommend specifying at least two DNS servers, otherwise DNS could become a single point of failure for your deployment.

You can specify up to three default DNS servers. These default DNS servers are used if there is no **Per-domain DNS server** defined for the domain being looked up.

- The TelePresence Conductor only queries one server at a time; if that server is not available the TelePresence Conductor will try another server from the list.

- The order that the servers are specified is not significant; the TelePresence Conductor attempts to favor servers that were last known to be available.

Per-domain DNS servers

In addition to the three default DNS servers, you can specify three additional explicit DNS servers for specified domains. This can be useful in deployments where specific domain hierarchies need to be routed to their explicit authorities.

For each additional per-domain DNS server address you can specify up to two **Domain names**. Any DNS queries under those domains are forwarded to the specified DNS server instead of the default DNS servers.

You can specify redundant per-domain servers by adding an additional per-domain DNS server address and associating it with the same **Domain names**. In this scenario, DNS requests for those domains will be sent in parallel to both DNS servers.

Tip: you can also use the DNS lookup tool (**Maintenance > Tools > Network utilities > DNS lookup**) to check which domain name server (DNS server) is responding to a request for a particular hostname.

Time

The **Time** page (**System > Time**) is used to configure the TelePresence Conductor's NTP servers and specify your local time zone.

Configuring the NTP servers

An NTP server is a remote server with which the TelePresence Conductor synchronizes in order to ensure its time is accurate. The NTP server provides the TelePresence Conductor with UTC time.

Accurate time is necessary for correct system operation.

Note: it is essential for a TelePresence Conductor to have access to an NTP server if it is in a cluster of other TelePresence Conductors.

To configure the TelePresence Conductor with one or more NTP servers to be used when synchronizing system time, enter up to five **Address**es in one of the following formats, depending on the system's DNS settings. (You can check these settings on the **DNS** page, **System > DNS**):

- if there are no **DNS servers** configured, you must use an IP address for the NTP server
- if there are one or more **DNS servers** configured, you can use an FQDN or IP address for the NTP server
- if there is a DNS **Domain name** configured in addition to one or more **DNS servers**, you can use the server name, FQDN or IP address for the NTP server.

To configure the authentication method to use with the individual NTP servers use one of the following options for the **Authentication** field:

Authentication method	Description
Disabled	No authentication method
Private key	Private key authentication. Using this method automatically generates a private key in the background, with which messages sent to the NTP server are authenticated.

Authentication method	Description
Symmetric key	Symmetric key authentication. When using this method the **Key ID**, **Hash** method and **Pass phrase** need to be specified. The values must match exactly the values on the NTP server. More than one NTP server can be configured to have the same combination of values. If a different **Pass phrase** is specified, the Key ID must also be unique and cannot be the same value as any Key ID already used on this device.

Displaying NTP status information

The synchronization status between the NTP server and the TelePresence Conductor is shown in the **Status** area as follows:

- *Starting*: the NTP service is starting.
- *Synchronized*: the TelePresence Conductor has successfully obtained accurate system time from an NTP server.
- *Unsynchronized*: the TelePresence Conductor is unable to obtain accurate system time from an NTP server.
- *Down*: the TelePresence Conductor's NTP client is not running.
- *Reject*: the NTP service is not accepting NTP responses.

Note that updates may take a few minutes to be displayed in the status table.

Other status information available includes:

Field	Description
NTP server	The actual NTP server that has responded to the request. This may be different to the NTP server in the NTP server address field.
Condition	Gives a relative ranking of each NTP server. All servers that are providing accurate time are given a status of *Candidate*; of those, the server that the TelePresence Conductor considers to be providing the most accurate time and is therefore using shows a status of *sys.peer*.
Flash	A code giving information about the server's status. `00 ok` means there are no issues. See the Flash status word reference table for a complete list of codes.
Authentication	Indicates the status of the current authentication method. One of *ok*, *bad* or *none*. *none* is specified when the **Authentication** method is *Disabled*.
Event	Shows the last event as determined by NTP (for example *reachable* or *sys.peer*)
Reachability	Indicates the results of the 8 most recent contact attempts between the TelePresence Conductor and the NTP server, with a tick indicating success and a cross indicating failure. The result of the most recent attempt is shown on the far right. Each time the NTP configuration is changed, the NTP client is restarted and the **Reachability** field will revert to all crosses apart from the far right indicator which will show the result of the first connection attempt after the restart. However, the NTP server may have remained contactable during the restart process.
Offset	The difference between the NTP server's time and the TelePresence Conductor's time.
Delay	The network delay between the NTP server and the TelePresence Conductor.

Field	Description
Stratum	The degree of separation between the TelePresence Conductor and a reference clock. `1` indicates that the NTP server is a reference clock.
Ref ID	A code identifying the reference clock.
Ref time	The last time that the NTP server communicated with the reference clock.

For definitions of the remaining fields on this page, and for further information about NTP, see Network Time Protocol website.

TelePresence Conductor time display and time zone

Local time is used throughout the web interface. It is shown in the system information bar at the bottom of the screen and is used to set the timestamp that appears at the start of each line in the Event Log.

Note: a UTC timestamp is included at the end of each entry in the Event Log.

Internally, the TelePresence Conductor maintains its system time in UTC. It is based on the TelePresence Conductor's operating system time, which is synchronized using an NTP server if one is configured. If no NTP servers are configured, the TelePresence Conductor uses its own operating system time to determine the time and date.

Specifying your local **Time zone** lets the TelePresence Conductor determine the local time where the system is located. It does this by offsetting UTC time by the number of hours (or fractions of hours) associated with the selected time zone. It also adjusts the local time to account for summer time (also known as daylight saving time) when appropriate.

SNMP

The **SNMP** page (**System > SNMP**) is used to configure the TelePresence Conductor's SNMP settings.

Tools such as Cisco TelePresence Management Suite (TMS) or HP OpenView may act as SNMP Network Management Systems (NMS). They allow you to monitor your network devices, including the TelePresence Conductor, for conditions that might require administrative attention.

The TelePresence Conductor supports the most basic MIB-II tree (.1.3.6.1.2.1) as defined in *RFC 1213*.

The information made available by the TelePresence Conductor includes the following:

- system uptime
- system name
- location
- contact
- interfaces
- disk space, memory, and other machine-specific statistics

By default, SNMP is *Disabled*, therefore to allow the TelePresence Conductor to be monitored by an SNMP NMS (including TMS), you must select an alternative **SNMP mode**. The configurable options are:

Field	Description	Usage tips
SNMP mode	Controls the level of SNMP support. *Disabled*: no SNMP support. *v3 secure SNMP*: supports authentication and encryption. *v3 plus TMS support*: secure SNMPv3 plus non-secure access to OID 1.3.6.1.2.1.1.2.0 only. *v2c*: non-secure community-based SNMP.	If you want to use secure SNMPv3 but you also use TMS as your external manager, you must select *v3 plus TMS support*.
SNMP community name	The TelePresence Conductor's SNMP community name. The default is *public*.	Only applies when using *v2c* or *v3 plus TMS support*.
System contact	The name of the person who can be contacted regarding issues with the TelePresence Conductor. The default is *Administrator*.	The **System contact** and **Location** are used for reference purposes by administrators when following up on queries.
Location	Specifies the physical location of the TelePresence Conductor.	
Username	The TelePresence Conductor's SNMP username, used to identify this SNMP agent to the SNMP manager.	Only applies when using *v3 secure SNMP* or *v3 plus TMS support*
v3 Authentication settings (only applicable to SNMPv3)		
Authentication mode	Enables or disables SNMPv3 authentication.	
Type	The algorithm used to encrypt authentication credentials. *SHA*: Secure Hash Algorithm. *MD5*: Message-Digest algorithm 5. The default is *SHA*.	
Password	The password used to encrypt authentication credentials.	Must be at least 8 characters.
v3 Privacy settings (only applicable to SNMPv3)		
Privacy mode	Enables or disables SNMPv3 encryption.	
Type	The security model used to encrypt messages. *DES*: Data Encryption Standard 56-bit encryption. *AES*: Advanced Encryption Standard 128-bit encryption. The default is *AES*.	
Password	The password used to encrypt messages.	Must be at least 8 characters.

The TelePresence Conductor does not support SNMP traps or SNMP sets, therefore it cannot be managed via SNMP.

Note: SNMP is disabled by default, because of the potentially sensitive nature of the information involved. Do not enable SNMP on a TelePresence Conductor on the public internet or in any other environment where you do not want to expose internal system information.

Managing conference bridges

You must configure the TelePresence Conductor with one or more pools of conference bridges that it can use to host the conferences it creates. The TelePresence Conductor periodically monitors all conference bridges in each of its pools for availability and resource usage. Upon receipt of a conference alias request from a VCS, the TelePresence Conductor checks the resource availability of the preferred conference bridge pool. It creates a conference on the conference bridge with the most available ports, cascading the conference to other conference bridges in the pool if and when required. If the preferred conference bridge pool can not be used, it will check the availability of the conference bridges in the pool that is the next highest preference.

This section includes the following topics:

Creating conference bridge pools

Each conference bridge must belong to a conference bridge pool. A single conference bridge can only belong to one pool. A single conference bridge pool can contain up to 30 conference bridges. Each TelePresence Conductor (or cluster of TelePresence Conductors) can use up to 30 conference bridges across all of its pools. For example, you could have a single pool with 30 conference bridges, or one pool with six conference bridges plus two pools with 12 conference bridges each.

To create a conference bridge pool:

1. Go to the **Conference bridge pools** page (**Conference configuration > Conference bridges > Conference bridge pools**).
   You will see a list of any existing conference bridge pools.
2. Click **New**.
   Enter the details of the new pool. The configurable options are:

Field	Description
Pool name	Descriptive name of the conference bridge pool.
Description	A free-form description of the conference bridge pool.
Conference bridge type	The type of conference bridges that can be assigned to this pool. All conference bridges within a pool must be of the same type and have the same configuration. This release of the TelePresence Conductor supports *Cisco TelePresence MCUs* only. Future versions may support other types of conference bridges.
Raise conference bridge resource alarm	Determines whether or not an alarm will be raised when the quantity of conference bridge ports being used and requested within this conference bridge pool exceeds a given percentage of the total quantity of ports available across all conference bridges in this pool. By default an alarm will be raised when 80% of ports are in use. For more information see Setting the threshold for raising conference bridge port usage alarms

3. Click **Create pool**.
   A new section **Conference bridges in this pool** will appear.

To add conference bridges to the pool, click **Add conference bridge**.

To save the new conference bridge pool, click **Save**.

Adding and editing conference bridges

Each TelePresence Conductor (or cluster of TelePresence Conductors) can use up to 30 conference bridges across all of its pools. For example, you could have a single pool with 30 conference bridges, or one pool with six conference bridges plus two pools with 12 conference bridges each.

A single conference bridge can only belong to one conference bridge pool.

Before adding a conference bridge, ensure that:

- you configure your conference bridges for use with the TelePresence Conductor
- all conference bridges in all pools are configured identically. Failure to do so will result in unpredictable behavior.
- all conference bridges used by the TelePresence Conductor are reserved for its exclusive use and are not used by any other system, for example Codian Conference Director

When editing the configuration of conference bridges, be aware that new conferences may not be connected, as the conference bridge will temporarily be unreachable. We therefore recommend you to edit conference bridges at off-peak times.

If a conference bridge is not available, the TelePresence Conductor will wait for a set period of time before attempting to re-contact it. This period is configurable on the **Conference bridge retry interval** page (**Conference configuration > Conference bridges > Conference bridge retry interval**).

To add a new conference bridge to a pool:

1. Go to the **Conference bridge pools** page (**Conference configuration > Conference bridges > Conference bridge pools**, then click on the name of the pool to which you wish to add a conference bridge.
   You will see a list of conference bridges (if any) currently belonging to the pool.
2. Click **Add conference bridge**.

When adding or editing a conference bridge, the configurable options are:

Field	Description
Name	Descriptive name of the conference bridge. For ease of reference, we recommend that you use the same name for the conference bridge both here and when Adding each conference bridge as a neighbor zone.
Description	A free-form description of the conference bridge.
State	Determines whether the TelePresence Conductor will treat this conference bridge as available for use. *Enabled*: the conference bridge will be used as and when required. *Disabled*: the conference bridge will not be used for any new conferences.

Field	Description
IP address or FQDN	The IP address or Fully Qualified Domain Name (FQDN) of the conference bridge. We strongly recommend that you use IP addresses in this field to ensure best performance.
Protocol	The protocol (either *HTTP* or *HTTPS*) that the TelePresence Conductor will use when communicating with the conference bridge. Note that because the conference bridge password is transmitted over the network, we recommend using HTTPS in deployments where interception of traffic between TelePresence Conductor and conference bridges could pose an unacceptable security risk. If you use HTTPS you must enable this feature on the conference bridge.
Port	The port on the conference bridge to which the TelePresence Conductor will connect. We recommend using *80* for HTTP and *443* for HTTPS.
Conference bridge username	The **User ID** of the account used by the TelePresence Conductor to log in to the conference bridge. This conference bridge account must have a **Privilege level** of *administrator*. See Configuring a conference bridge for use with the Conductor for information on how to create a new user for the TelePresence Conductor on the conference bridge. We do not recommend that the TelePresence Conductor uses the conference bridge's default admin user account.
Conference bridge password	The password used to log in to the conference bridge. This cannot be a blank password.
Dial plan prefix	The prefix that has been configured as part of a VCS search rule to route calls to this conference bridge. The prefix must be unique for each conference bridge in the pool. It is alphanumeric. **Note:** there must not be any conflict between any **Incoming alias** or **Conference name** (used when Creating and editing conference aliases), the Call Policy prefix, or Conference bridge dial plan prefixes, otherwise you may experience unpredictable behavior. For more information, see Avoiding dial plan conflicts. For more information on dial plans and prefixes, refer to Designing a dial plan. For more information on VCS search rule configuration, refer to Configuring a VCS search rule for each conference bridge.
Conference bridge type	The type of this conference bridge. This field cannot be modified. This release of the TelePresence Conductor supports *Cisco TelePresence MCUs* only. Future versions may support other types of conference bridges.
Conference bridge pool	The pool to which this conference bridge belongs. This field cannot be modified.
Dedicated content ports	Determines the number of dedicated content ports on the conference bridge. These content ports will be excluded from the calculation of how many ports to reserve. The default is 0.

Disabling conference bridges

Disabling a conference bridge will make it temporarily unavailable, preventing the TelePresence Conductor from using it for new conferences. When a conference bridge that is currently in use is disabled, any existing conferences on that conference bridge will be unaffected and new callers will still be able to join the existing conference.

During the time that a conference bridge is disabled, the TelePresence Conductor will still continue to poll it for information about its resources. For this reason we recommend that a conference bridge that is either no longer required by a TelePresence Conductor, or required for use by another system, be completely removed from the pool once all existing conferences have been completed.

To disable a conference bridge, temporarily preventing the TelePresence Conductor from using it:

1. Go to the **Conference bridge pools** page (**Conference configuration > Conference bridges > Conference bridge pools**).
2. Click on the name of the pool to which the conference bridge belongs.
3. Select the conference bridge you wish to remove.
4. Click **Disable**.

Deleting conference bridges

Note: deleting a conference bridge from the conference bridge pool removes the conference bridge completely. Any conference running on a conference bridge that is deleted will be torn down.

To permanently delete a conference bridge from the pool:

1. Go to the **Conference bridge pools** page (**Conference configuration > Conference bridges > Conference bridge pools**).
2. Click on the name of the pool to which the conference bridge belongs.
3. Select the conference bridge you wish to delete and click **Disable**.
4. Wait until all conferences on that conference bridge have finished (to check, go to **Status > Conference bridges**).
5. Go back to the **Conference bridge pools** page, select the conference bridge you wish to delete and click **Delete**.

Changing global conference bridge settings

Some settings on the TelePresence Conductor apply to all conference bridges in its pools. The **Global conference bridge settings** page (**Conference configuration > Conference bridges > Global conference bridge settings**) allows you to perform the following tasks:

- Changing the conference bridge retry interval
- Setting the threshold for raising conference bridge port usage alarms

Changing the conference bridge retry interval

The TelePresence Conductor constantly monitors its pool of conference bridges to check whether they are available. If a conference bridge is not contactable, the **Conference bridge retry interval** setting determines the number of seconds the TelePresence Conductor will wait before attempting to re-contact a conference bridge that was previously unavailable.

You can change this setting on the **Global conference bridge settings** page (**Conference configuration > Conference bridges > Global conference bridge settings**).

Note that if you set this interval too high, it will take a long time for the TelePresence Conductor to start using a conference bridge it has experienced a problem with. If you set this interval too low, and there is a

conference bridge with a persistent fault, the TelePresence Conductor will waste resource by trying to communicate with it.

The default is 300 seconds (5 minutes). You should not deviate from the default setting unless advised to do so by a Cisco Technical Support Representative.

Setting the threshold for raising conference bridge port usage alarms

The TelePresence Conductor constantly monitors all conference bridges in its pools to check the total number of ports that are available, and how many of those are currently in use.

By default, the TelePresence Conductor will raise an alarm when more than 80% of all the currently available ports are in use and when 80% of all available ports within a conference bridge pool are in use. The alarm raised is one of the following:

- MCU resource warning: MCU usage is approaching or has reached full capacity
- MCU pool resource warning: MCU pool usage is approaching or has reached full capacity

There are two situations when the alarm will be raised:

- When a new conference is created, or a new participant joins an existing conference, and this takes the port usage above the configured threshold. In this situation one of the above alarms will be raised but participants can continue to create and join conferences until there are no more ports available.
- When a conference could not be created because the number of required ports exceeded the number of ports currently available. The number of required ports for a conference is the total of all auto-dialed participants, reserved lecture ports, cascade ports, and reserved content ports. In this situation, an event will appear in the event log in addition to the above alarm. The event is **Not enough conference bridge resource to handle request**.

To change whether and when this alarm is raised:

1. Go to the relevant page
   - For all conference bridges go to **Global conference bridge settings** page (**Conference configuration > Conference bridges > Global conference bridge settings**)
   - For conference bridges within a pool go to the **Conference bridge pools** page (**Conference configuration > Conference bridges > Conference bridge pools**)
2. Choose one of these options:
   - to change the threshold at which alarms are raised, select the **Raise conference bridge resource alarm** check box, and in the **Threshold (%)** field enter the desired value
   - to only raise alarms when a conference could not be created because the number of required ports exceeded the number of ports currently available, select the **Raise conference bridge resource alarm** check box and in the **Threshold (%)** field enter a value of *100*
   - to never raise alarms, clear the **Raise conference bridge resource alarm** check box

After the alarm has been raised, it can be acknowledged by the system administrator. If the alarm has been acknowledged, it will be raised again if the resource usage still exceeds the configured threshold after 24 hours.

The alarm will not be lowered until the system is restarted. It will not be lowered automatically by the system if the current port usage drops back below the threshold.

Viewing all conference bridges across all pools

To view a list of all conference bridges currently being used by the TelePresence Conductor, go to the **All conference bridges** page (**Conference configuration > Conference bridges > View all conference bridges**).

From this page you can click on any of the column headings to sort the list by, for example, **Conference bridge pool**, **Address**, or **Dial plan prefix**.

To edit details of any of the conference bridges, for example to disable the conference bridge or change the pool to which it belongs, click on **View/Edit**.

Moving a conference bridge between pools

To move a conference bridge from one pool to another:

1. Go to the **Conference bridge** page for the conference bridge you want to move. You can access this page in two ways:
   - From the **Conference bridge pools** page **Conference configuration > Conference bridges > Conference bridge pools**, click on the **Pool name** of the pool to which the conference bridge belongs. This will take you to the **Conference bridge pools** page which lists all the conference bridges in that pool. Click on the **Name** of the conference bridge you want to move.
   - From the **All conference bridges** page (**Conference configuration > Conference bridges > View all conference bridges**), click on the **Name** of the conference bridge you want to move.
2. From the **Conference bridge pool** drop-down list, select the pool to which the conference bridge is to be moved.
3. Select **Save**.

Conference bridge response time

In networks with high latency or packet loss, a warning may be raised on the TelePresence Conductor indicating that the conference bridge has taken a long time to respond, seemingly indicating a fault on the conference bridge. However, there are several possible causes for this including:

- packet loss
- high network latency
- slow-running conference bridge (although this is actually the least likely cause)

The warning will be seen in the event log and will have the following data:

```
Event="An error occurred while communicating externally."

Detail="mcu response took <x> seconds. It should take no
longer than 1 second"

where 'x' is the number of seconds it took to respond.
```

About creating conferences

A conference is created when someone dials a pre-determined conference alias, e.g. **learn.math@example.com**. To enable this, you must first define the aliases that can be dialed, and the settings that will be applied to each conference when it is created.

To do this:

1. Ensure that all the VCSs and conference bridges you will be using with this TelePresence Conductor are working properly together and have been configured in accordance with the information in Configuring a VCS for use with the TelePresence Conductor and Configuring a conference bridge for use with the TelePresence Conductor.
2. Create one or more pools of conference bridges that the TelePresence Conductor will use for its conferences.
3. Add conference bridges to the pool. Each pool must contain at least one conference bridge.
4. Set up at least one Service Preference, defining the order in which conference bridge pools will be used if resources are limited.
5. Create a template for the conference. The template will determine whether the conference is a **meeting** (where all participants dial in using the same conference alias and have the same privileges) or a **lecture** (where the chairperson(s) and the guests dial in using different aliases and are given different privileges).
6. Define a conference alias for the conference. A single conference can have more than one alias, and lectures must have at least two aliases – one for the chairperson(s) and one for the guests.
7. Optionally, define any auto-dialed participants whom you want to be called by the conference bridge when the conference starts. These participants can be individual endpoints, FindMe IDs, or recording devices.

Examples

See Example - creating a meeting and Example - creating a lecture for full examples of how to configure the TelePresence Conductor.

Selecting the preferred conference bridges for a conference

For any particular conference, you can determine which conference bridge pools the TelePresence Conductor will attempt to use to host that conference, in order of preference. You do this by creating a Service Preference, and then assigning a Service Preference to a conference template.

A Service Preference is a prioritized list of conference bridge pools. If no conference bridges within the first pool can be used to host a conference (for example, if there are insufficient resources available for the requirements of the conference), the TelePresence Conductor will check whether the second pool in the list can be used, and so on.

A Service Preference can contain anywhere between 1 and 30 conference bridge pools.

A single conference bridge pool can be used in any number of Service Preferences.

Creating a Service Preference

To create a Service Preference:

1. Ensure that you have created all the conference bridge pools that you want to include in the Service Preference.
2. Go to the **Conference bridge Service Preferences** page (**Conference configuration > Conference bridges > Conference bridge Service Preferences**) and select **New**.
   You will be taken to the **Conference bridge Service Preference** page.
3. Enter details of the new Service Preference. The configurable options are:

Field	Description
Service Preference name	Descriptive name of the Service Preference. This name will appear in the **Conference bridge Service Preference** drop-down list when assigning the Service Preference to a template.
Description	A free-form description of the Service Preference.
Conference bridge type	The type of conference bridge that can be assigned to this Service Preference. All conference bridges within a pool, and all pools within a Service Preference, must be of the same type and have the same configuration. This release of the TelePresence Conductor supports *Cisco TelePresence MCUs* only. Future versions may support other types of conference bridges.

4. In the **Pools** section, from the drop-down list select the conference bridge pool that you want to be used first for any conferences that use this Service Preference.
5. Click **Add selected pool**.
   The new Service Preference will be saved, with the selected conference bridge pool as the first pool to be used.
6. To assign additional conference bridge pools to this Service Preference, select another conference bridge pool from the drop-down list and click **Add selected pool**.
7. To change the order of priority of the conference bridge pools you have selected, use the arrows in the **Change order** column.
8. Once all conference bridge pools have been added, click **Save**.

Cascading conferences across conference bridges and conference bridge pools

When a conference is **created**, the TelePresence Conductor will check the resources of the preferred conference bridge pool (according to the Service Preference for the template being used) and where possible, use one of the conference bridges in that pool to host the primary conference. If there are insufficient resources available within that pool, the TelePresence Conductor will then check the availability of the conference bridges in each of the other pools within that Service Preference, in order of priority, until it finds a conference bridge on which it can host the conference.

When an existing conference is **cascaded**, regardless of the conference bridge pool being used to host the primary conference, the TelePresence Conductor will first check the resources of the conference bridges in the preferred conference bridge pool and where possible, use one of the conference bridges in that pool to host the cascade. This could mean that a single conference is cascaded between conference bridges in different conference bridge pools.

Creating and editing conference templates

Conference templates define the settings to be applied to different conferences when they are created. The same template can be used by more than one conference alias.

The **Conference templates** page (**Conference configuration > Conference templates**) lists all the existing conference templates and allows you to edit, delete and create new templates.

When creating or editing a conference template, the configurable options are:

Field	Description
Modify conference template section	
Name	Descriptive name of the conference template.
Description	A free-form description of the conference template.
Conference type	Determines the nature of the conference that will be created when this template is used. ■ *Meeting*: the conference will have one type of participant, and all participants will be given the same priority. ■ *Lecture*: there will be two different types of participants with different levels of priority. Each participant type will use a different alias to dial in to the conference.
No. of chairperson ports to reserve	(Available when **Type** is *Lecture*) The number of ports to be reserved on the conference bridge for use by chairpersons in the conference. One port per chairperson will be required. The chairperson port will be reserved on the primary conference bridge. See About port reservation for more information.
Call Policy mode	Determines whether you want to check whether users who have dialed a conference alias that uses this template have the right to create a conference. *Off*: no checks will be made. *On*: the TelePresence Conductor will check the VCS's Call Policy before allowing users to create a conference. **Note:** if set to *On*, you must also configure the TelePresence Conductor's Call Policy prefix. See Using Call Policy for more information.
Conference bridge Service Preference	Allows you to select a Service Preference that this template will use. A Service Preference is a prioritized list of conference bridge pools that the TelePresence Conductor will use for this conference. You must create your Service Preferences before you can create a template. For more information see Selecting the preferred conference bridges for a conference.

Field	Description
No. of cascade ports to reserve	The number of ports to be reserved on the primary conference bridge for connections to additional conference bridges. These ports will be used if the conference exceeds the capacity of the primary conference bridge and is cascaded to one or more conference bridges. Each connection between the primary conference bridge and an additional conference bridge requires one port. If you want to prevent a conference from cascading across multiple conference bridges, you can set the number of cascade ports to reserve to 0. If you do so, be aware that this may prevent new participants from being able to join a conference. For more information about cascade ports, see About port reservation For more information about cascading across conference bridges, see Cascading conferences across conference bridges and conference bridge pools
Limit number of participants	Determines whether there will be a limit set on the total number of participants permitted in this conference. This number includes all auto-dialed participants (i.e. participants who are dialed in to the conference by the conference bridge) and all ad hoc participants (i.e. participants who dial in to the conference, including those who have been assigned a reserved Chairperson port). The maximum number of participants must be more than the total number of auto-dialed participants plus reserved Chairperson ports. For more information see Limiting the number of participants in a conference.
Limit the conference duration (minutes)	Determines whether there will be a limit set on the maximum duration of conferences created using this template. When selected, specify the limit of the conference duration in minutes. Depending on the configuration of the conference bridge, there will be warnings issued - as an audio notification and/or as overlaid text - at varying intervals before the conference is about to end. See What warnings do I get on a Cisco TelePresence MCU that my conference is finishing? for information on how to turn the warnings off, and on the intervals at which the warnings will be displayed.
Advanced section	
Conference layout	The conference layout to use in all conferences that are created using this template. The layout specifies how the screen is divided up into panes to display the participants in a conference. It applies when there are more than two participants in the conference. The default is to use the **Default view family** that has been configured on the Cisco MCU. We strongly recommend that you use this default in order to ensure a consistent user experience. (As described in Configuring a conference bridge for use with the TelePresence Conductor, all conference bridges must be configured identically for this and all other settings.) ■ To change the layout, click **Choose layout** and select the desired layout from the pop-up screen. ■ To use the Cisco MCU's **Default view family**, select  . For more information on conference layouts see *Understanding how participants display in layout views* in the *Cisco TelePresence MCU Online Help*.
Participant PIN	The PIN needed to access a meeting-type conference. This PIN applies to all conferences created using this template.
Chair PIN	The PIN needed to access a lecture-type conference as the chairperson/lecturer. This PIN applies to all conferences created using this template. Note that for Cisco MCU version 4.2 you need to specify both PIN and guest PIN when using PINs.
Guest PIN	The PIN needed to access a lecture-type conference as the guest/student. This PIN applies to all conferences created using this template.

Field	Description
Parameters to pass on to primary MCU	Additional configuration parameters to pass to the primary Cisco MCU when the conference is created. There are two methods of selecting parameters to pass on to the primary Cisco MCU: ■ Click **New** and select the desired option(s) from the drop-down box. ■ Click **Advanced** and enter JSON directly into this field. **Note:** this feature is for advanced use only. See Parameters to pass on to MCUs for more information.
Parameters to pass on to cascade MCU	Additional configuration parameters to pass to secondary Cisco MCUs when the conference is cascaded. To add a new parameter, click **New** and select the desired option from the drop-down box. You can also enter JSON directly into this field by clicking **Advanced**. **Note:** this feature is for advanced use only. See Parameters to pass on to MCUs for more information.
Allow content	Whether or not participants will be able to send content video such as a presentation. *Yes*: a single port will be reserved on the primary conference bridge and each cascade conference bridge specifically for content. *No*: participants will not be able to send content, regardless of the number of ports available on the conference bridge. See Content port for more information.

About port reservation

Note: the reservation of different types of ports on the TelePresence Conductor, as described below, is independent of the **Media port reservation** setting on the Cisco MCUs, which should be set to *Disabled*.

Each conference is hosted on one conference bridge, known as the primary conference bridge. When the TelePresence Conductor receives a request to create a new conference, it checks the resources available on all the conference bridges in the preferred pool to determine which conference bridge should host the conference. Before deciding which conference bridge to use, the TelePresence Conductor must know how many ports that conference will require, so it can assign the conference to a conference bridge that has sufficient resources.

Chairperson ports

A conference can have more than one chairperson. All chairpersons in the conference must be able to connect directly to ports on the primary conference bridge. Each chairperson will require at least one port, which will be used to send and receive audio and video.

If there are not enough ports available on the conference bridge when a chairperson tries to connect to the conference, they will not be able to join. To ensure that there are enough ports available for all chairpersons to join the conference, when creating a conference template you are asked how many ports the TelePresence Conductor should reserve on the primary conference bridge for chairpersons. For the duration of the conference, these ports will be reserved solely for the use of chairpersons.

Note: if the conference requires more chairperson ports than have been reserved, a chairperson may still be able to connect to the conference but only if the primary conference bridge has sufficient ports available.

Cascade ports

If a conference exceeds the capacity of the primary conference bridge, the TelePresence Conductor will bring in another conference bridge and use its resources as well - this is known as cascading. If the second conference bridge then runs out of resources, the conference will be cascaded from the primary conference bridge to a third conference bridge, and so on.

Each cascade (from the primary conference bridge to another conference bridge) will use one port on the primary conference bridge. If there is no port available, the conference cannot be cascaded and any further participants will not be able to join the conference. To ensure that there are enough ports available for the conference to be cascaded to as many conference bridges as required, when creating a conference template you are asked how many ports the TelePresence Conductor should reserve on the primary conference bridge for cascades to other conference bridges in the event that the conference needs to be cascaded. For the duration of the conference, these ports will be reserved solely for the use of cascades.

It can be difficult to determine the correct number of cascade ports to reserve. If you reserve more cascade ports than are needed, you may end up "wasting" resources on the primary conference bridge. Conversely, if you reserve fewer ports than are needed, the conference may not be able to grow to the required size (especially when the network is heavily loaded).

If you want to prevent a conference from cascading across multiple conference bridges, you can set the number of cascade ports to reserve to 0. If you do so, be aware that this may prevent new participants from being able to join a conference.

Note: if the conference requires more cascade ports than have been reserved, it will not be cascaded.

Content port

Conference participants may want to send content video such as a presentation. Such content may require a separate port on the conference bridge. To permit participants to send content, you must select the option to **Allow content**. This reserves a port on the primary conference bridge and each cascade conference bridge specifically for content. Any participant can send content using these ports, but only one participant at a time can send content.

The number of **Dedicated content ports** specified on the conference bridge is excluded from the calculation of how many ports to reserve for content.

Note: if you have not selected the option to **Allow content**, participants will **not** be able to send content, regardless of the number of ports available on the conference bridge.

Parameters to pass on to MCUs

CAUTION: this feature is for advanced use only.

Cisco TelePresence MCUs support the *Cisco TelePresence MCU Remote Management API*. This API enables third-party control of the Cisco MCU via messages sent using the XML-RPC protocol. It is this API that the TelePresence Conductor uses to manage conferences on the Cisco MCUs in its pool.

The TelePresence Conductor allows you to make use of the `conference.create` call of this API through the **Parameters to pass on to primary MCU** and **Parameters to pass on to cascade MCU** fields of the

Conference templates page (**Conference configuration > Conference templates > New**). Messages in these fields are passed on to the Cisco MCU when a conference is created, and allow you to specify Cisco MCU-based parameters for the conference such as the MCU template, PIN, layout, and mute settings.

You can enter messages into these fields in two ways: using the basic drop-down menu, or the advanced option of entering valid JSON directly into the input field. These two options are described in the following sections.

When a conference is created on a Cisco MCU, the settings for that conference will depend on the MCU template being used. However, settings configured via the **Parameters to pass on to MCU** fields on the TelePresence Conductor will override any settings specified by the MCU template.

For full information on using the Cisco MCU API, including the parameters that can be set using the `conference.create` call, see *Cisco TelePresence MCU Series API Reference Guide*.

Basic input

To use the basic drop-down menu to enter messages:

1. From within the input field, click **New**. (If this is not visible, click **Basic** to the right of the input field.)
2. From the drop-down list, select the parameter you wish to use, and click **Add**.
   The name of the selected parameter appears on the left, with options to **Delete** or **Edit** on the right.
3. To set a value for the parameter, click **Edit**. Enter the desired value into the input box that appears, and click **OK**.
4. To add additional parameters, repeat the steps above.

Advanced input

CAUTION: if messages are not in correct JSON format, this can result in the conference or cascade failing to be created or a Cisco MCU becoming temporarily unusable and excluded from the pool of available conference bridges.

To use JSON to enter messages:

1. Click **Advanced** to the right of the input field.
   An input field appears. If you have already used the **Basic** option to set any parameters, these will appear within the field in JSON format.
2. Enter the desired message in valid JSON format.

Do not use the following parameters. These are used by the TelePresence Conductor and changing them will result in a failure to create conferences:

- `conferenceName`
- `numericId`
- `guestNumericId`
- `startTime`
- `maximumAudioPorts`
- `reservedAudioPorts`
- `maximumVideoPorts`
- `reservedVideoPorts`
- `repetition`

- **weekday**
- **whichWeek**
- **weekDays**
- **terminationType**
- **terminationDate**
- **numberOfRepeats**

We also advise that you do not use the following parameters, which may also result in a failure to create conferences:

- **cleanupTimeout**
- **contentMode (do not use when running MCU version 4.2)**
- **contentContribution**

The TelePresence Conductor does not perform in-depth checking of data in these fields. Any incorrect configuration of the settings may result in your conference failing to be created (or in a cascade failing to be created) and perhaps in a Cisco MCU becoming temporarily unusable and excluded from the pool of available conference bridges.

Example - selecting an MCU template and allowing the conference to remain when a chairperson leaves

In this example we want to ensure that the conference remains in place when the last Chairperson has left, and we also want to use a specific MCU template for the conference.

Field	Input
Parameters to pass on to primary MCU	{"lastChairmanLeavesDisconnect": false,"templateNumber": 0}
Parameters to pass on to cascade MCU	{"lastChairmanLeavesDisconnect": false,"templateNumber": 0}

Example

The following example shows a conference template for an all-hands conference that has 2 presenters and up to 250 participants.

For full examples showing how to set up conference templates as part of creating meetings and lectures, see Example - creating a meeting and Example - creating a lecture.

Field	Input	Explanation
Name	Sales and Marketing all hands	This is the name that will appear in the web interface for this template.
Description	Template for sales and marketing all hands presentations	Descriptions are optional but helpful if you are managing many templates.

Field	Input	Explanation
Conference type	*Lecture*	The type of conference we are setting up is a lecture.
No. of cascade ports to reserve	5	The conference has up to 250 participants and we expect that 5 additional MCUs will be needed to host the conference. See About port reservation for more information.
No. of chairperson ports to reserve	2	Each chairperson will require one port for audio and video. This conference has 2 chairpersons (the Sales Vice President and the Marketing Vice President). See About port reservation for more information.
Call Policy mode	*Off*	We do not want to check whether users who have dialed a conference alias that uses this template have the right to create a conference.
Conference bridge Service Preference	Select the Service Preference you want to use	A Service Preference is a prioritized list of conference bridge pools that will be used to host the conference. Conference bridge pools and Service Preferences must be set up before any templates can be configured.
Maximum number of participants	260	There will be up to 250 guest participants, plus the 2 chairpersons, plus the device being used to record the conference, making a total of 253. We enter 260 to ensure all these participants can dial in and there is some spare capacity.
Conference layout		Leave as the default.
Parameters to pass on to primary MCU		Leave this field blank.
Parameters to pass on to cascade MCU		Leave this field blank.
Allow content	*Yes*	The chairpersons will be sending content in the form of a presentation.

Limiting the number of participants in a conference

You can limit the total number of participants in a conference. The total number of participants to which the limit applies includes all auto-dialed participants (i.e. participants who are dialed in to the conference by the conference bridge) plus all ad hoc participants. (Ad hoc participants are those who dial in to the conference using one of the conference aliases. They include participants who have been assigned one of the reserved Chairperson ports.) The number of participants does not include any ports reserved for content or cascades.

- To place a limit on the number of participants, select the **Limit number of participants** check box and in the **Maximum** field, enter the total number of participants for the conference.
- If you do not want to place a limit on the number of participants, clear the **Limit number of participants** check box.

The default is for no limit.

The maximum number of participants must be higher than:

- the total number of auto-dialed participants associated with the template, plus
- all the participants for whom a port has been reserved (i.e. the setting in the **No. of chairperson ports to reserve** field for lectures).

This is to ensure that all these participants will be able to access the conference. If the maximum number of participants is not higher than these two numbers added together, the conference will not be created.

The reason that the maximum number of participants must be more than (rather than equal to) the number of auto-dialed and reserved participants is because a conference is not created until the first ad hoc participant dials in, so the conference already has one participant when it is created. You must therefore set the maximum number of participants to a value that will allow the first ad hoc participant, plus all auto-dialed and reserved Chairperson participants, plus any additional ad hoc participants, to dial in to the conference.

You will receive a warning in any of the following situations:

- an auto-dialed participant is assigned to an existing template, and doing so means that the number of auto-dialed participants plus reserved Chairperson ports is equal to or higher than the maximum
- the number of reserved Chairperson ports is changed, and doing so means that the number of auto-dialed participants plus reserved Chairperson ports is equal to or higher than the maximum
- the maximum number of participants is changed to a number that is equal to or lower than the current number of auto-dialed participants plus reserved Chairperson ports.

Creating and editing conference aliases

A Conference alias maps dialed aliases to conferences using regular expressions and specifies the user's role in the conference (participant, chairperson, or guest).

When configuring each conference alias, you must specify the template to use for the conference, the name of the conference, and whether that user will be admitted to the conference as a participant, chairperson or guest. To create or join a conference, an endpoint user must dial a specified alias.

The **Conference aliases** page (**Conference configuration > Conference aliases**) lists all the existing conference aliases and allows you to edit, delete and create new conference aliases.

For meetings, you must configure at least one conference alias. However, you can set up two or more aliases for the same conference.

For lectures, you must configure at least two conference aliases - one for the chairperson and one for guests.

Note: there must not be any conflict between any **Incoming alias** or **Conference name**, the Call Policy prefix, or Conference bridge dial plan prefixes, otherwise you may experience unpredictable behavior. For more information, see Avoiding dial plan conflicts.

Conference aliases use regular expressions, allowing you to use pattern matching and wildcards to specify the alias that users dial to access the conference, and the name of the conference when it is created on the conference bridge.

- For more information about regular expressions, refer to About regular expressions.
- For specific examples of how regular expressions can be used to set up conference aliases refer to Regular expression examples - conference aliases and Regular expression examples - lectures.

When creating or editing a conference alias, the configurable options are:

Field	Description
Name	Descriptive name of the conference alias.
Description	A free-form description of the conference alias.
Incoming alias (must use regex)	A regular expression (regex) that matches one or more aliases that a user can dial to access a conference.
Conference name (must use regex replace string)	A regular expression (regex) replace string that defines how the **Incoming alias** will be modified to result in the conference name. This will be the same conference name that is then used on the conference bridge. We recommend that you use conference names that are 31 characters or fewer. See Conference name length for more information.
Priority	Assigns a priority to the conference alias. The priority must be unique for each conference alias. The priority is used if the alias that has been dialed matches the **Incoming alias** of more than one conference alias. In such cases, the conference alias with the highest priority (closest to 1) will be used. If the alias that was dialed matches only one conference alias, the **Priority** won't be used but is still a required field.
Conference template	The template that is used when the conference is created. This will determine whether the conference is a *Meeting* or a *Lecture*, and thus what **Role names** will be available in the following field.
Role name	Determines the privileges that will be assigned to a caller dialing in to the conference using this conference alias. The options that are available are determined by the settings of the **Conference template** that has been selected in the previous field. *Participant* (available when the template **Type** is *Meeting*): the caller will join the conference as a chairperson participant. *Chairperson* (available when the template **Type** is *Lecture*): the caller will join the conference as a chairperson participant. *Guest* (available when the template **Type** is *Lecture*): the caller will join the conference as a guest participant. See About Chairperson and Guest roles for more information on the differences between the two roles.

Conference name length

Cisco TelePresence MCUs currently support conference names of up to 31 characters. If the TelePresence Conductor has a conference name that is 32 characters or more it will hash the name and pass the hash value to the Cisco MCU for it to use as the conference name. The TelePresence Conductor will continue to use the original name itself.

If a conference name is longer than 32 characters, you can view the hashed value on the **Conferences status** page (**Status > Conferences**):

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

To avoid hashing, we recommend that you use conference names that are 31 characters or fewer. You will need to carefully consider any regular expressions that you use in the **Conference name** field to ensure that all resulting conference names do not exceed this length.

Example

The following example shows a conference alias used by the two Vice-Presidents presenting an all-hands conference to 250 members of the sales and marketing team.

For full examples showing how to set up conference aliases for meetings and lectures, see Example - creating a meeting and Example - creating a lecture.

Field	Input	Explanation
Name	VP all hands	This is the name that will appear in the web interface for this conference alias.
Description	Alias used by VPs to dial into all hands conferences.	Descriptions are optional but helpful if you are managing many aliases.
Incoming alias (must use regex)	show\.allhands	This regex specifies that users must dial **`show.allhands`** exactly to join the conference. The full stop (**`.`**) is a special regex character that matches any single character. The backslash (**`\`**) escapes this special character. In combination they mean that only an actual full stop will be matched. Without the use of the backslash, this regex would match not only **`show.allhands`** but also any string starting with **`show`** followed by any single character followed by **`allhands`**, e.g. **`showxallhands`** or **`show9allhands`**. For more information, see About regular expressions.
Conference name (must use regex replace string)	allhands	This is the name of the conference as it will appear on the conference bridge. The same **Conference name** must be configured for the Guest alias. In this example, if there is a match with the incoming alias then exactly this string will be used for the conference name, regardless of the actual incoming alias. However, if you have used brackets as part of the incoming alias regex to group sets of characters together, you can use the characters **`\1`**, **`\2`**, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Priority	50	Priority can be from *1* (highest) to *65535*. Assigning a priority of *50* and adding other priorities in increments of 10 gives us plenty of scope to add other aliases of higher or lower priority.
Conference template	*Sales and Marketing all hands*	This is the name we gave the template created in Step 1 of the example on how to create a lecture. It appears in the drop-down list along with all other template names.
Role name	*Chairperson*	This conference alias is to be used by the presenters only. The conference bridge will give them Chairperson privileges when they join the conference.

Creating and editing auto-dialed participants

Auto-dialed participants are addresses that are automatically dialed by the conference bridge(s) when a conference starts. The address could relate to a device such as an endpoint or recording device, or could be a FindMe ID.

Each auto-dialed participant is associated with a **Conference template** and **Conference name match**. Whenever a conference is created using the specified **Conference template**, the resulting conference name is compared with the **Conference name match**. If there is a match, the conference bridge will automatically dial the specified participant. In this sense the Conference name acts as a filter, so that only conferences using a specific template and with a specific name will have the auto-dialed participant added.

The **Auto-dialed participants** page (**Conference configuration > Auto-dialed participants**) lists all the existing auto-dialed participants and allows you to edit, delete and create new participants.

When creating or editing an auto-dialed participant, the configurable options are:

Field	Description
Name	Descriptive name of the auto-dialed participant.
Description	A free-form description of the auto-dialed participant.
Conference template	The template that, when used, will cause this participant to be dialed in to the conference (if there is a match with the conference name).
Conference name match (must use regex)	The conference to which this participant will be added. You must use a regular expression (regex) that can match one or more conference names. Participants will be added to the conference only if the conference name matches the regular expression. The default for this field is `(.*)`, which is a regular expression that will match against all possible conference names. This will result in the **Address** being dialed for all conferences created using the specified **Conference template**.
Participant address	The address that is automatically dialed by the conference bridge when a matching conference starts. You can enter an explicit auto-dialed participant address, or a regular expression that is used to produce the auto-dialed participant address. If using a regular expression, the `\n` notations (`\1`, `\2`, and so on) are replaced by the bracketed portions of the **Conference name match** field. Note that SIP addresses must include the domain (in other words, be in the format `address@example.com`).
Protocol	Determines the protocol that the conference bridge will use to call this participant. The options are *H.323* or *SIP*.

Field	Description
Role type	Determines the privileges that will be assigned to the participant when it is dialed in to the conference by the conference bridge. The options that are available are determined by the settings of the **Conference template** that has been selected: *Participant* (available when the template **Type** is *Meeting*): the caller will join the conference as a chairperson. *Chairperson* (available when the template **Type** is *Lecture*): the caller will join the conference as a chairperson. *Guest* (available when the template **Type** is *Lecture*): the caller will join the conference as a guest. For more information on the differences between the two roles, see About Chairperson and Guest roles
DTMF sequence	Specifies a series of DTMF tones that will be sent by the conference bridge to the auto-dialed participant after the call has been connected. This feature can be used where the auto-dialed participant is a device such as an audio bridge that has an audio menu navigated by DTMF. There is a two second pause after the call connects after which the conference bridge will send the DTMF tones, which are sent one every half second. The DTMF sequence can include the digits **0**-**9** and the characters ***** and **#**. It can also include a comma (**,**), which represents a two-second pause. You can insert as many additional two-second pauses as you want. For more information about using DTMF, see Sending DTMF tones to an auto-dialed participant.
Keep conference alive	Determines whether or not the conference will end when all other participants have left the conference. *Yes*: the conference will keep running when only this auto-dialed participant remains. *No*: the conference will automatically end when only this auto-dialed participant remains. Beware that: ■ if the auto-dialed participant is an endpoint that cannot terminate a call itself, such as a recording device (for example a TelePresence Content Server or ISDN), you must select *No*. Selecting *Yes* will result in the conference never being terminated. ■ if the auto-dialed participant is an ISDN endpoint that has been set to auto-answer, selecting *Yes* may result in an unexpectedly high ISDN bill. ■ this setting will be ignored if the conference bridge parameter **lastChairmanLeavesDisconnect** is set to *true* and this auto-dialed participant's **Role type** is set to *Guest*.
Conference layout	The conference layout to use for this auto-dialed participant. The layout specifies how the screen is divided up into panes to display the participants in a conference. It applies when there are more than two participants in the conference. The default is *None*, which does not send any conference layout information to the Cisco MCU. We strongly recommend that you use this default in order to ensure a consistent user experience. The option *default* specifically tells the Cisco MCU to use the default layout view configured on it. The option *family1* is an example of a layout family and the option *layout1* is an example of a specific layout. For a list of the layout families and specific layouts available on the Cisco MCU with images, see Conference layouts. For more information on conference layouts see *Understanding how participants display in layout views* in the *Cisco TelePresence MCU Online Help*.

Field	Description
Additional parameters	Additional parameters to pass to the auto-dialed participant when the conference is created. To add a new parameter, click **New** and select the desired option from the drop-down box. You can also enter JSON directly into this field by clicking **Advanced**. **Note:** this feature is for advanced use only. Incorrect usage can lead to the auto-dialed participant being unavailable.
State	Determines whether calls will be made to this auto-dialed participant when a conference is created using the selected template.

Using auto-dialed participants and Multiway

When planning to use Multiway with TelePresence Conductor, refrain from adding auto-dialed participants that are or could be using Multiway. Only add devices that can be trusted not to use Multiway, such as for example recording servers or audio bridges.

Example

If you define the rendezvous conference **`meet.ben@domain.com`** with the auto-dialed participant **`ben@domain.com`**, you need to ensure that

- **either** **`ben@domain.com`**'s endpoint has Multiway disabled,
- **or** Ben must promise not to use the Multiway call flows.

Sending DTMF tones to an auto-dialed participant

If the auto-dialed participant is a device such as an audio bridge that has an audio menu navigated by DTMF, you can use the **DTMF sequence** field to specify a series of DTMF tones to send to the device after the call has been connected.

Example

You want the conference bridge to dial out to a PIN-protected audio conference on an audio bridge. The conference ID is **`555`** and the PIN is **`888`**. The audio bridge requires that you press **`#`** after entering the ID and after entering the PIN.

In this example you would set the **DTMF sequence** to be **`555#,,888#`**. The two commas represent a four second pause which allows the audio bridge's automated menu system time to process the ID and request the PIN.

What if an auto-dialed participant can't be reached?

Sometimes the call to the auto-dialed participant might not be successful (for example, if the participant is busy or does not answer). You can control what a conference bridge does in such situations by going to the conference bridge's **Conference settings** page (**Settings > Conferences**) and in the **Advanced settings** section, selecting one of the following options from the **Failed preconfigured participants redial behavior** field:

CAUTION: each conference bridge must be configured identically for this and all other settings. Failure to do so will result in unpredictable behavior.

Never redial	The conference bridge will never attempt to redial the participant, even if they fail to connect.
Default	The conference bridge will make nine retry attempts to the participant. The first four attempts will be at one minute intervals; the following five attempts will be at five minute intervals.
Constant redial	The conference bridge will make constant retry attempts to the participant. The first four attempts will be at one minute intervals; all redial attempts after this will be at five minute intervals.

Example - automatically recording a conference

The following example shows how we can use the auto-dialed participant feature to automatically record all Sales and Marketing all-hands conferences. We do this by creating an auto-dialed participant with an address that routes to our Cisco TelePresence Content Server recording device.

Note: for full examples showing how to set up auto-dialed participants as part of creating meetings and lectures, see Example - creating a meeting and Example - creating a lecture.

Field	Input	Explanation
Name	Record all hands	This is the name that will appear in the web interface for this auto-dialed participant.
Description	Records all hands conferences on the sales TCS	Descriptions are optional but helpful if you are managing many auto-dialed participants.
Conference template	*Sales and Marketing all hands*	This is the name we gave the template created in Step 1 of the example on how to create a lecture. It appears in the drop-down list along with all other template names.
Conference name match	allhands	This regex specifies that the name of the conference must be *allhands*. For more information, see About regular expressions. This means that whenever a conference is created that uses the *Sales and Marketing all hands* template and has a name of *allhands*, the **address** below will be automatically dialed.
Participant address	record.allhands	This address will be dialed by the conference bridge when the conference starts. We have set up our network so that this address routes to our Cisco TelePresence Content Server and creates a recording. In this example, if there is a match with the conference name, then exactly this string will be dialed. However, if you have used brackets as part of the incoming **Conference name match** regex to group sets of characters together, you can use the characters \1, \2, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Protocol	H.323	The *record.allhands* address is an H.323 ID, so we want the conference bridge to dial it using this protocol.
Role type	Guest	The address is for a recording device which does not need any special privileges in the conference, so we select *Guest*.

Field	Input	Explanation
DTMF sequence		Leave this field blank.
Keep conference alive	No	When all other callers have left the conference, the recording device will still be in the call. We do not want the call to continue at this point.
Conference layout	None	Leave this field as *None*.
Additional parameters		Leave this field blank.
State	Enabled	We want to use this auto-dialed participant straight away, so we leave the default of *Enabled*.

Example - automatically adding a person to a conference

The following example shows how we can use the auto-dialed participant feature to automatically add Alice to all Sales team meetings. We do this by placing a call to her FindMe ID, **alice.findme**.

Note: for full examples showing how to set up auto-dialed participants as part of creating meetings and lectures, see Example - creating a meeting and Example - creating a lecture.

Field	Input	Explanation
Name	Alice	This is the name that will appear in the web interface for this auto-dialed participant.
Description	Alice's FindMe ID	Descriptions are optional but helpful if you are managing many auto-dialed participants.
Conference template	Sales team	This is the name we gave the template created in Step 1 of the example on how to create a meeting. It appears in the drop-down list along with all other template names.
Conference name match	(.*)	This default regular expression will match against all conference names. This means that whenever the *Sales team* conference template is used to create a conference, the **Address** specified below will be dialed, regardless of the actual conference name. For more information see About regular expressions.
Participant address	alice.findme	This is Alice's FindMe ID. It will be dialed by the conference bridge when the conference starts. In this example, exactly this string will be used for the address, regardless of the actual conference name. However, if you have used brackets as part of the **Conference name match** regex to group sets of characters together, you can use the characters `\1`, `\2`, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Protocol	H.323	The *alice.findme* address is an H.323 ID, so we want the conference bridge to dial it using this protocol.
Role type	Participant	The template being used is for a meeting, so *Participant* is the only option available.
DTMF sequence		Leave this field blank.

Field	Input	Explanation
Keep conference alive	Yes	Alice may want to remain in the conference when all the other participants have left, perhaps if she wants to ask other participants to dial in to the conference.
Conference layout	None	Leave this field as *None*.
Additional parameters		Leave this field blank.
State	Enabled	We want to use this auto-dialed participant straight away, so we leave the default of *Enabled*.

About Chairperson and Guest roles

Conference bridges have two types of conference participant: **Chairperson** and **Guest**. A conference can have more than one Chairperson.

In general, a Chairperson has more control over a conference than a Guest, and a conference can be set up so that it starts and ends depending on whether or not a Chairperson is present.

Assigning roles

When a user joins a conference on a conference bridge via the TelePresence Conductor, they will have either a Chairperson or Guest role assigned to them based on how they joined the conference:

- If they joined by dialing a conference alias, they will be given the role associated with that alias. See Creating and editing conference aliases for more information.
- If they joined the conference because they were dialed in by the conference bridge as an auto-dialed participant, they will be given the role assigned to that participant. See Creating and editing auto-dialed participants for more information.

Note: meetings can only have one type of participant, so all meeting participants are given a role of Chairperson.

Differences between Chairperson and Guest roles

The options available to **Chairperson** and **Guest** participants are determined by the conference bridge. Some options are configurable on the conference bridge but others are not. The differences are described below.

Starting the conference

A conference will not begin until the first Chairperson joins. Guests who join a conference before the first Chairperson has joined will see a black screen with the on-screen text *Waiting for conference chairperson*. There will be no audio, apart from an audio prompt after five seconds and every minute thereafter.

This behavior is not configurable.

Ending the conference

You can control the behavior when the last Chairperson leaves the conference using the **When only guests remain** template setting on the Cisco MCU.

This setting can be modified via the parameter **lastChairmanLeavesDisconnect** within the fields **Parameters to pass on to primary MCU** and **Parameters to pass on to cascade MCU** (if applicable) under **Conference configuration > Conference template**.

The two options are:

- *true* (default) - all remaining guests will be disconnected
- *false* - all participants may continue the conference until the last one disconnects

The option *true* should only be set when the TelePresence Conductor's **Conference template** has a **Conference type** of *Lecture*.

Beware that if the MCU parameter **lastChairmanLeavesDisconnect** is set to *true* then any auto-dialed participant with **Role type** of *Guest* will be disconnected when all other non-guest participants have left the conference. This applies even if **Keep conference alive** is set to *Yes*.

For more information see Parameters to pass on to MCUs.

Taking the chair

Only a Chairperson can "take the chair". On "taking the chair", a participant can:

- nominate a "broadcaster"; that is, they can choose which participant's video will be sent to all other participants in "1 x 1 view" (full-screen view)
- decide to disconnect any other participant(s)

This behavior is not configurable.

Note: "taking the chair" is only supported for H.323 calls and only if floor and chair control has been enabled on the MCU. Not all endpoints support the H.243 floor and chair control functionality.

Conference layout in automatic lecture mode

When automatic lecture mode is configured on the Cisco MCUs, there is a difference in the conference layout for chairpersons and guests. The chairpersons see their custom layout, whereas guests see only the chairperson who is currently speaking.

For more information on automatic lecture mode see *Understanding how participants display in layout views* in the *Cisco TelePresence MCU Online Help*.

Example - creating a meeting

This example shows how to set up the TelePresence Conductor to enable the five members of the Sales team to create or join a team meeting by dialing **meet.sales**. Alice, the head of Sales, is automatically dialed in to all these team meetings.

Prerequisites

This example assumes that you have already:

- Configured the TelePresence Conductor with a pool of conference bridges.
- Configured the VCS to route the alias **meet.sales** to this TelePresence Conductor. See Configuring a VCS for use with the TelePresence Conductor for more information.
- Configured each conference bridge appropriately. See Configuring a conference bridge for use with the TelePresence Conductor for more information.

Step 1 - create a template

From the **Conference templates** page (**Conference configuration > Conference templates**), click **New** and create a template for the meeting with the following parameters:

Field	Input	Explanation
Name	Sales team	This is the name that will appear in the web interface for this template.
Description	Template for sales team meetings	Descriptions are optional but helpful if you are managing many templates.
Conference type	*Meeting*	The type of conference we are setting up is a meeting.
No. of cascade ports to reserve	0	The meeting has only 5 participants so it is unlikely to use up all the ports on the primary conference bridge.
Call policy mode	*Off*	We do not want to check whether users who have dialed a conference alias that uses this template have the right to create a conference.
Conference bridge Service Preference	Select the Service Preference you want to use	A Service Preference is a prioritized list of conference bridge pools that will be used to host the conference. Conference bridge pools and Service Preferences must be set up before any templates can be configured.
Maximum number of participants	6	There will be a total of 6 participants - the 5 members of the sales team, plus Alice.
Conference layout		Leave as the default.
Parameters to pass on to primary MCU		Leave this field blank.
Parameters to pass on to cascade MCU		Leave this field blank.
Allow content	Select *Yes*	These meetings often involve team members giving presentations.

Step 2 - configure a conference alias

From the **Conference aliases** page (**Conference configuration > Conference aliases**), click **New** and configure a conference alias for the meeting with the following parameters:

Field	Input	Explanation
Name	Sales team meeting	This is the name that will appear in the web interface for this conference alias.
Description	Alias to dial for sales team meetings	Descriptions are optional but helpful if you are managing many aliases.
Incoming alias	meet\.sales	This regex specifies that users must dial **`meet.sales`** exactly to join the conference. The full stop (**`.`**) is a special regex character that matches any single character. The backslash (**`\`**) escapes this special character. In combination they mean that only an actual full stop will be matched. Without the use of the backslash, this regex would match not only **`meet.sales`** but also any string starting with **`meet`** followed by any single character followed by **`sales`**, e.g. **`meetxsales`** or **`meet9sales`**. For more information, see About regular expressions.
Conference name	sales	This is the name of the conference as it will appear on the conference bridge. In this example, if there is a match with the incoming alias then exactly this string will be used for the conference name, regardless of the actual incoming alias. However, if you have used brackets as part of the incoming alias regex to group sets of characters together, you can use the characters **`\1`**, **`\2`**, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Priority	100	Priority can be from *1* (highest) to *65535*. Assigning a priority of *100* gives us plenty of scope to add other aliases of higher or lower priority.
Conference template	*Sales team*	This is the name we gave the template created in Step 1. It appears in the drop-down list along with all other template names.
Role name	*Participant*	Everyone who dials in to a meeting will have a role of Participant, meaning the conference bridge will give them equal privileges.

Step 3 - define any auto-dialed participants

This is an optional step and can be used to prompt the conference bridge to dial a particular endpoint, recording device or alias whenever a conference is created. In this example we want the conference bridge to automatically dial Alice's FindMe ID whenever there is a Sales team meeting.

From the **Auto-dialed participants** page (**Conference configuration > Auto-dialed participants**), click **New** and enter the following parameters:

Field	Input	Explanation
Name	Alice	This is the name that will appear in the web interface for this auto-dialed participant.
Description	Alice's FindMe ID	Descriptions are optional but helpful if you are managing many auto-dialed participants.
Conference template	Sales team	This is the name we gave the template created in Step 1. It appears in the drop-down list along with all other template names.

Field	Input	Explanation
Conference name match	(.*)	This default regular expression will match against all conference names. This means that whenever the *Sales team* conference template is used to create a conference, the **Address** specified below will be dialed, regardless of the actual conference name. For more information see About regular expressions.
Participant address	alice.findme	This is Alice's FindMe ID. It will be dialed by the conference bridge when the conference starts. In this example, exactly this string will be used for the address, regardless of the actual conference name. However, if you have used brackets as part of the **Conference name match** regex to group sets of characters together, you can use the characters `\1`, `\2`, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Protocol	H.323	The *alice.findme* address is an H.323 ID, so we want the conference bridge to dial it using this protocol.
Role type	Participant	The template being used is for a meeting, so *Participant* is the only option available.
DTMF sequence		Leave this field blank.
Keep conference alive	Yes	Alice may want to remain in the conference when all the other participants have left, perhaps if she wants to ask other participants to dial in to the conference.
Conference layout	None	Leave this field as *None*.
Additional parameters		Leave this field blank.
State	Enabled	We want to use this auto-dialed participant straight away, so we leave the default of *Enabled*.

Example - creating a lecture

This example shows how to set up the TelePresence Conductor to enable the Sales Vice President and the Marketing Vice President to give a joint presentation to all 250 members of the sales and marketing teams. To access the conference, the VPs dial **show.allhands** and the rest of the team dials **watch.allhands**. The conference is automatically recorded.

Prerequisites

This example assumes that you have already:

- Configured the TelePresence Conductor with a pool of conference bridges.
- Configured the VCS to route the aliases **show.allhands** and **watch.allhands** to this TelePresence Conductor. See Configuring a VCS for use with the TelePresence Conductor for more information.
- Configured each conference bridge appropriately. See Configuring a conference bridge for use with the TelePresence Conductor for more information.

Step 1 - create a template

From the **Conference templates** page (**Conference configuration > Conference templates**), click **New** and create a template for the presentation with the following parameters:

Field	Input	Explanation
Name	Sales and Marketing all hands	This is the name that will appear in the web interface for this template.
Description	Template for sales and marketing all hands presentations	Descriptions are optional but helpful if you are managing many templates.
Conference type	*Lecture*	The type of conference we are setting up is a lecture.
No. of cascade ports to reserve	5	The conference has up to 250 participants and we expect that 5 additional MCUs will be needed to host the conference. See About port reservation for more information.
No. of chairperson ports to reserve	2	Each chairperson will require one port for audio and video. This conference has 2 chairpersons (the Sales Vice President and the Marketing Vice President). See About port reservation for more information.
Call Policy mode	*Off*	We do not want to check whether users who have dialed a conference alias that uses this template have the right to create a conference.
Conference bridge Service Preference	Select the Service Preference you want to use	A Service Preference is a prioritized list of conference bridge pools that will be used to host the conference. Conference bridge pools and Service Preferences must be set up before any templates can be configured.
Maximum number of participants	260	There will be up to 250 guest participants, plus the 2 chairpersons, plus the device being used to record the conference, making a total of 253. We enter 260 to ensure all these participants can dial in and there is some spare capacity.
Conference layout		Leave as the default.
Parameters to pass on to primary MCU		Leave this field blank.
Parameters to pass on to cascade MCU		Leave this field blank.
Allow content	*Yes*	The chairpersons will be sending content in the form of a presentation.

Step 2 - configure a conference alias for the chairpersons

From the **Conference aliases** page (**Conference configuration > Conference aliases**), click **New** and configure a conference alias to be used by the Sales Vice President and the Marketing Vice President with the following parameters:

Field	Input	Explanation
Name	VP all hands	This is the name that will appear in the web interface for this conference alias.
Description	Alias used by VPs to dial into all hands conferences.	Descriptions are optional but helpful if you are managing many aliases.
Incoming alias (must use regex)	show\.allhands	This regex specifies that users must dial **`show.allhands`** exactly to join the conference. The full stop (**`.`**) is a special regex character that matches any single character. The backslash (**`\`**) escapes this special character. In combination they mean that only an actual full stop will be matched. Without the use of the backslash, this regex would match not only **`show.allhands`** but also any string starting with **`show`** followed by any single character followed by **`allhands`**, e.g. **`showxallhands`** or **`show9allhands`**. For more information, see About regular expressions.
Conference name (must use regex replace string)	allhands	This is the name of the conference as it will appear on the conference bridge. The same **Conference name** must be configured for the Guest alias. In this example, if there is a match with the incoming alias then exactly this string will be used for the conference name, regardless of the actual incoming alias. However, if you have used brackets as part of the incoming alias regex to group sets of characters together, you can use the characters **`\1`**, **`\2`**, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Priority	50	Priority can be from *1* (highest) to *65535*. Assigning a priority of *50* and adding other priorities in increments of 10 gives us plenty of scope to add other aliases of higher or lower priority.
Conference template	*Sales and Marketing all hands*	This is the name we gave the template created in Step 1. It appears in the drop-down list along with all other template names.
Role name	*Chairperson*	This conference alias is to be used by the presenters only. The conference bridge will give them Chairperson privileges when they join the conference.

Step 3 - configure a conference alias for the guests

From the **Conference aliases** page (**Conference configuration > Conference aliases**), click **New** and configure a conference alias to be used by the members of the sales and marketing teams with the following parameters:

Field	Input	Explanation
Name	team all hands	This is the name that will appear in the web interface for this conference alias.
Description	Alias used by team to dial into all hands conferences	Descriptions are optional but helpful if you are managing many aliases.
Incoming alias (can use regular expression)	watch.allhands	Users must dial exactly this alias to join the conference. If you want to use wildcards in this field, see About regular expressions.
Conference name (can use regular expression)	allhands	This is the name of the conference as it will appear on the conference bridge. The same **Conference name** must be configured for the Chairperson alias. If you have used a regular expression in the **Incoming alias** field, you can also use one here to transform the alias into a conference name. See About regular expressions for more information.
Priority	60	Priority can be from *1* (highest) to *65535*. Assigning a priority of *60* and adding other priorities in increments of 10 gives us plenty of scope to add other aliases of higher or lower priority.
Conference template	*Sales and Marketing all hands*	This is the name we gave the template created in Step 1. It appears in the drop-down list along with all other template names.
Role name	*Guest*	This conference alias is to be used by team members only. The conference bridge will give them Guest privileges when they join the conference.

Step 4 - define any auto-dialed participants

This is an optional step and can be used to prompt the conference bridge to dial a particular endpoint, recording device or alias whenever a conference is created. In this example we will use the auto-dialed participant functionality to automatically record the conference.

From the **Auto-dialed participants** page (**Conference configuration > Auto-dialed participants**), click **New** and enter the following parameters:

Field	Input	Explanation
Name	Record all hands	This is the name that will appear in the web interface for this auto-dialed participant.
Description	Records all hands conferences on the sales TCS	Descriptions are optional but helpful if you are managing many auto-dialed participants.
Conference template	*Sales and Marketing all hands*	This is the name we gave the template created in Step 1. It appears in the drop-down list along with all other template names.

Field	Input	Explanation
Conference name match	allhands	This regex specifies that the name of the conference must be *allhands*. For more information, see About regular expressions. This means that whenever a conference is created that uses the *Sales and Marketing all hands* template and has a name of *allhands*, the **address** below will be automatically dialed.
Participant address	record.allhands	This address will be dialed by the conference bridge when the conference starts. We have set up our network so that this address routes to our Cisco TelePresence Content Server and creates a recording. In this example, if there is a match with the conference name, then exactly this string will be dialed. However, if you have used brackets as part of the incoming **Conference name match** regex to group sets of characters together, you can use the characters \1, \2, etc. to reuse these as part of this replace string. For more information, see About regular expressions.
Protocol	H.323	The *record.allhands* address is an H.323 ID, so we want the conference bridge to dial it using this protocol.
Role type	Guest	The address is for a recording device which does not need any special privileges in the conference, so we select *Guest*.
DTMF sequence		Leave this field blank.
Keep conference alive	No	When all other callers have left the conference, the recording device will still be in the call. We do not want the call to continue at this point.
Conference layout	None	Leave this field as *None*.
Additional parameters		Leave this field blank.
State	Enabled	We want to use this auto-dialed participant straight away, so we leave the default of *Enabled*.

Using Call Policy

About Call Policy

When Call Policy is in use, the TelePresence Conductor will check with the Cisco TelePresence Video Communication Server (VCS) to determine whether a user who is attempting to create a particular conference has the right to do so. Call Policy is enabled on per-template basis, and requires a **Call Policy prefix** to be configured on the TelePresence Conductor. It also requires an appropriate Call Policy to be configured on the VCS.

Note: there must not be any conflict between any **Incoming alias** or **Conference name** (used when Creating and editing conference aliases), the Call Policy prefix, or Conference bridge dial plan prefixes, otherwise you may experience unpredictable behavior. For more information, see Avoiding dial plan conflicts.

When to use VCS or TelePresence Conductor Call Policy

The TelePresence Conductor's Call Policy works in conjunction with the VCS's Call Policy and allows you to distinguish between those users you want to permit to **create** a conference based on a particular template, and those you want to permit to **join** the conference. Whether you use Call Policy on the VCS only, or on both the VCS and TelePresence Conductor depends on the desired result, as follows:

- **To prevent a user from creating or joining any conferences:** use VCS Call Policy only, so that the request never reaches the TelePresence Conductor.
- **To prevent a user from creating a particular conference, but allow them to join the existing conference:** enable Call Policy on the TelePresence Conductor in conjunction with an appropriate Call Policy on the VCS, as per the information in this section.
- **To allow a user to create and join a conference:** Call Policy is not required on the TelePresence Conductor or VCS.

Note: when Call Policy is enabled on the TelePresence Conductor, it applies only to users attempting to create a conference that does not already exist. After the conference has been created (by a user who is allowed to dial the prefix), a user who previously dialed the conference alias and had their call rejected because they did not have the right to create the conference will be able to dial the same conference alias and successfully join the conference.

Defaults

The default **Call Policy prefix** is **create.**. If no **Call Policy prefix** is configured, Call Policy on the TelePresence Conductor will not work, so this field cannot be left blank.

Note: in numeric dial plans, this field will need to be changed.

Configuring Call Policy

To use Call Policy on the TelePresence Conductor:

1. Enable or disable Call Policy on a per-template basis using the **Call Policy mode** setting on the **Conference templates** page (**Conference configuration > Conference templates**).
2. If any templates are using Call Policy, then you must configure the TelePresence Conductor with a prefix to use. This is done using the **Call Policy prefix** setting on the **Call Policy** page (**Conference configuration > Call Policy**). The same prefix is used for all templates that have Call Policy enabled.
3. Configure the VCS with an appropriate Call Policy that will allow only those users permitted to create conferences to place calls that start with the **Call Policy prefix**. See *Cisco TelePresence Video Communication Server Administrator Guide* and *Cisco TelePresence Conductor Deployment Guide* for more information.

Example usage

In the following example:

- the TelePresence Conductor has been configured with a conference alias of **meet.alice** which creates a conference with the name **alice**
- the **meet.alice** alias uses a template that has Call Policy enabled
- the TelePresence Conductor's **Call Policy prefix** is **create.**.
- the VCS is configured with a Call Policy that says Alice is the only person allowed to dial **create.meet.alice**

Call not allowed

Ben dials **meet.alice**.

The VCS forwards the request to the TelePresence Conductor.

The TelePresence Conductor looks up the **meet.alice** alias and sees that the conference name for that alias is **alice**. It then checks to see whether the **alice** conference already exists. It does not, so it adds the Call Policy prefix (**create.**) to the conference alias that it received and sends the resulting string (**create.meet.alice**) back to the VCS.

The VCS checks its Call Policy to see whether Ben is allowed to dial **create.meet.alice**. He is not, so the VCS rejects the call.

Call allowed

Alice dials **meet.alice**.

The VCS forwards the request to the TelePresence Conductor.

The TelePresence Conductor looks up the **meet.alice** alias and sees that the conference name for that alias is **alice**. It then checks to see whether the **alice** conference exists. It does not, so it adds **create.** to the conference alias and sends the resulting string (**create.meet.alice**) back to the VCS.

The VCS checks its Call Policy to see whether Alice is allowed to dial **create.meet.alice**. She is, so the VCS forwards the request for **create.meet.alice** to the TelePresence Conductor.

When the TelePresence Conductor receives a conference alias that begins with the same string as the **Call Policy prefix**, it interprets this as approval from the VCS to create the associated conference. So when it receives **create.meet.alice** it strips the **create.** prefix, looks up the resulting **meet.alice** conference alias and follows the settings for that alias to create the conference **alice**, with Alice as the first participant.

Ben then dials **meet.alice**.

The VCS forwards the request to the TelePresence Conductor.

The TelePresence Conductor looks up the **meet.alice** alias and sees that the conference name for that alias is **alice**. It then checks to see whether the **alice** conference already exists. It does, so Ben is allowed to join Alice in the **alice** conference.

About user accounts

The options under the **Users** menu allow you to configure the usernames and passwords of users logging in to the TelePresence Conductor.

The Administrator account page allows you to configure the username and password of a single administrator user account. These account credentials can be used by an administrator to log in to the TelePresence Conductor web interface, by the Cisco TelePresence Video Communication Server when accessing the TelePresence Conductor policy service, or by third party applications such as Cisco TelePresence Management Suite (TMS) to access the TelePresence Conductor.

The LDAP configuration page allows you to configure the TelePresence Conductor to use LDAP to obtain account authentication credentials from a remote server.

The Administrator groups page allows you to set the access levels for users belonging to administrator groups provided by the remote server.

There is also a Root account which can be used to log in to the TelePresence Conductor operating system but should not be used in normal operation.

Note: it is extremely important to configure a secure password for the root account in order to restrict SSH access.

Administrator account

The **Administrator accounts** page (**Users > Administrator accounts**) allows you to configure the username and password of a single administrator user account. These account credentials can be used by an administrator to log in to the TelePresence Conductor web interface, by the Cisco TelePresence Video Communication Server when accessing the TelePresence Conductor policy service, or by third party applications such as Cisco TelePresence Management Suite (TMS) to access the TelePresence Conductor.

The administrator account can only be used when the **Administrator authentication source** on the **LDAP configuration** page has been set to *Local only* or *Both*.

Note: the default password for the administrator user is **TANDBERG**. The TelePresence Conductor's conference functionality will be disabled until this password has been changed. It is important to select a secure password for the administrator user.

Changing the administrator username

Note: the username and password for the administrator account is replicated across peers in a cluster. Therefore if you change the username or password on one peer, it will be changed on all other peers.

To change the username used to log in to the TelePresence Conductor as an administrator:

1. Go to the **Administrator accounts** page (**Users > Administrator accounts**).
2. Select **View/Edit**.
3. In the **Username** field, enter the name to be used by the administrator when logging in.
4. Select **Save**.

Changing the administrator password

Note: the username and password for the administrator account is replicated across peers in a cluster. Therefore if you change the username or password on one peer, it will be changed on all other peers.

To change the password used to log in to the TelePresence Conductor as an administrator:

1. Log in to the TelePresence Conductor as the administrator.

   Note: if you have forgotten the administrator account password, see Resetting forgotten passwords for instructions on how to reset it.

2. Go to the **Administrator accounts** page (**Users > Administrator accounts**).
3. Select **View/Edit**.
4. In the **Password** field, enter the password to be used by the administrator when logging in.
   The **Password strength** box next to the field will indicate how secure your chosen password is.
5. In the **Confirm password** field, re-enter the password.
6. Select **Save**.

Password strength

When entering passwords, the bar next to the **Password** field changes color to indicate the complexity of the password.

Note: you cannot set blank passwords for the administrator account.

LDAP configuration

The **LDAP configuration** page (**Users > LDAP configuration**) allows you to configure the TelePresence Conductor to use LDAP to obtain account authentication credentials from a remote server.

Note: the Administrator account can still be used to log in to the TelePresence Conductor even if LDAP is being used for remote account authentication.

The configurable options are:

Field	Description
LDAP configuration: this section allows you to enable or disable the use of LDAP for remote account authentication.	

Field	Description
Administrator authentication source	Defines where administrator login credentials are authenticated against an external credentials directory such as Active Directory. *Local only*: credentials are verified against a local database stored on the system. *Remote only*: credentials are verified against an external credentials directory. *Both*: credentials are verified first against a local database stored on the system, and then if no matching account is found the external credentials directory is used instead. The default is *Local only*. Note that you cannot log in using the **admin** account if *Remote only* authentication is in use.
LDAP server configuration: this section specifies the connection details to the LDAP server.	
Server address	The IP address or Fully Qualified Domain Name (or server address, if a DNS Domain Name has also been configured) of the LDAP server to use when making LDAP queries.
FQDN address resolution	Sets how the LDAP **Server address** is resolved if it is specified as an FQDN. *Address record*: DNS A record lookup. *SRV record*: DNS SRV record lookup. The default is *Address record*.
Port	Sets the IP port of the LDAP server to use when making LDAP queries. Typically, non-secure connections use *389* and secure connections use *636*.
Encryption	Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS). *TLS*: uses TLS Encryption for the connection to the LDAP server. *Off*: no encryption is used. The default is *Off*.
Authentication configuration: this section specifies the authentication credentials the TelePresence Conductor will use when binding to the LDAP server.	
Bind DN	The user Distinguished Name used by the TelePresence Conductor when binding to the LDAP server.
Bind password	The password used by the TelePresence Conductor when binding to the LDAP server. The maximum plaintext length is 60 characters, which is then encrypted.
SASL	The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. *None*: no mechanism is used. *DIGEST-MD5*: the DIGEST-MD5 mechanism is used. The default is *DIGEST-MD5*.
Bind username	The username to use when binding to the LDAP server. Only applies if using SASL.

Field	Description
Directory configuration: this section specifies the base distinguished names to use when searching for account and group names.	
Base DN for accounts	The distinguished name to use as the base when searching for administrator and user accounts.
Base DN for groups	The distinguished name to use as the base when searching for administrator and user groups. **Note:** if no **Base DN for groups** is specified, then the Base DN for accounts will be used for both groups and accounts.

The status of the connection to the specified LDAP server is displayed at the bottom of the page.

Administrator groups

If you are using a remote server for authentication of users, you must use the administrator groups that have been set up on that server to determine the levels of access assigned to administrators after they have been successfully authenticated to use the TelePresence Conductor.

If an administrator belongs to more than one group, it is assigned the highest level permission for each of the three access settings (**Access**, **Web access** and **API access**) across all of its groups

If a user does not belong to any administrator groups listed on this page, they will not be able to log in.

If remote authentication is being used then all groups that are applicable must be listed here.

The **Administrator groups** page (**Users > Administrator groups**) allows you to set the access levels for users belonging to administrator groups provided by the remote server.

When creating or editing administrator groups, the configurable options are:

Field	Description
Name	The name of the administrator group that has been set up on the remote authentication server.
State	Determines whether access to the TelePresence Conductor is enabled or disabled for members of the specified administrator group. *Enabled*: members of this group can access the TelePresence Conductor. *Disabled*: access will be denied to members of this group. **Note:** if a user belongs to more than one administrator group with a combination of both *Enabled* and *Disabled* states, their access will be *Enabled*.
Access	The access level given to members of the specified administrator group. *Read-write*: configuration can be viewed and changed. *Read-only*: configuration can be viewed but not changed. **Note:** if a user belongs to more than one administrator group with a combination of *Read-write* and *Read-only* access levels, they will be assigned the higher level.
Web access	Determines whether users in this group are allowed to log onto the system using the web interface.

Field	Description
API access	Determines whether users in this group are allowed to access the system's status and configuration using the Application Programming Interface (API).

Root account

The TelePresence Conductor provides a root account which can be used to log in to its operating system. This account has a username of **root** (all lower case) and a default password of **TANDBERG** (all upper case).

For security reasons you must change the password as soon as possible. Conference functionality is disabled and an alarm is displayed on the web interface until the **root** password is changed from the default.

Note: the **root** account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the Administrator account instead.

Changing the root account password

To change the password for the **root** account:

1. Log in to the TelePresence Conductor as **`root`**. By default you can only do this using a serial connection or SSH.

   Note: if you have forgotten the **root** account password, see Resetting forgotten passwords for instructions on how to reset it.

2. Type **`passwd`**.
   You will be asked for the new password.
3. Enter the new password and when prompted, retype the new password.
   You will receive the message:
   `passwd: password updated successfully`
4. Type **`exit`** to log out of the root account.

Enabling and disabling access over SSH

By default, the root account can be accessed over either a serial connection or SSH.

To enable and disable access to the root account using SSH:

1. Log in to the TelePresence Conductor as **`root`**.
2. Type one of the following commands:
   - **`rootaccess -s on`** to enable access using SSH
   - **`rootaccess -s off`** to disable access using SSH
3. Type **`exit`** to log out of the root account.

If you have disabled SSH access while logged in using SSH, your current session will remain active until you log out, but all future SSH access will be denied. The only way you can then re-enable SSH access is to log in using a serial connection and run the **`rootaccess -s on`** command.

Resetting forgotten passwords

Note: the username and password for the administrator account is replicated across peers in a cluster. Therefore if you change the username or password on one peer, it will be changed on all other peers.

The root account password is not replicated across peers.

Resetting your root or admin password via a serial connection

If you have forgotten the password for either the administrator account or the **root** account, you can reset it using the following procedure:

1. Connect a PC to the TelePresence Conductor using the serial cable as per the instructions in the *Cisco TelePresence Conductor Getting Started Guide*.
2. Restart the TelePresence Conductor.
3. Log in from the PC with the username **`pwrec`**. No password is required.
4. When prompted, select the account (*root* or *admin*) whose password you want to change.
5. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a restart. After that time you will have to restart the system again to change the password.

Resetting your admin password if you still have access to the root account

If you have still got access to the **root** account, but you have forgotten your password for the **administrator** account, you can reset the admin password using the following procedure:

1. Log in to the **root** account via a serial connection or SSH.
2. Enter the command **`passwd admin`**.
3. When prompted enter the new password twice.

About the Status menu

The **Status** menu allows you to view the status of the following items:

- Getting a status overview
- Alarms
- Conference bridge status
- Conferences status
- Conference participants
- Event Log

Getting a status overview

The **Overview** page **Status > Overview** gives an overview of the current status of the TelePresence Conductor.

The following information is displayed:

Field	Description	Notes
System host name	The name that has been assigned to the TelePresence Conductor by the system administrator.	This setting is configured on the **DNS** page (**System > DNS**).
IPv4 address	The TelePresence Conductor's IPv4 address.	This setting is configured on the **IP** page (**System > IP**).
Up time	The amount of time that has elapsed since the system last rebooted.	Restarting the system does not affect the system up time.
Product	This will be Cisco TelePresence Conductor.	
Hardware serial number	The serial number of the hardware on which the TelePresence Conductor software is installed.	
Software version	The version of software that is currently installed on the TelePresence Conductor.	To upgrade to a new version of software, refer to About upgrading software components.
Software build	The build number of this software version.	
Software release date	The date on which this version of the software was released.	
Number of conference bridges	The number of conference bridges that have been configured on the TelePresence Conductor. The list of conference bridges can be viewed and edited on the **All conference bridges** page (**Conference configuration > Conference bridges > View all conference bridges**).	For further information about each conference bridge, go to the **Conference bridge status** page (**Status > Conference bridges**). See Managing conference bridges for more information regarding conference bridges.

Field	Description	Notes
Number of active conferences	The number of conferences currently taking place.	For further information about each conference, go to the **Conferences status** page (**Status > Conferences**).

Alarms

Alarms occur when an event or configuration change has taken place on the TelePresence Conductor that requires some manual administrator intervention, such as a restart. Alarms may also be raised for hardware and environmental issues such as faulty disks and fans or high temperatures.

For a list of the alarm categories that can appear on the TelePresence Conductor, see Alarm categories.

Viewing alarms

The **Alarms** page (**Status > Alarms**, or by clicking on the red Alarm icon which appears at the top right of any page when an alarm is in place) provides a list of all the alarms currently in place on your system (and, in the **Action** column where applicable, their proposed resolution). If your system is part of a cluster, this page will display all alarms across all peers in the cluster.

Actioning alarms

CAUTION: You should not run a system with unresolved alarms because functionality and performance may be affected.

You should deal with each alarm immediately by clicking each **Action** and making the necessary configuration changes to resolve the problem.

If you are experiencing any problems with the TelePresence Conductor, the first step should be to investigate and fix any active alarms.

If your system is part of a cluster, you should action each alarm on the peer to which it relates. The **Action** hyperlink will redirect you to the relevant peer. You may see multiple copies of the same alarm disappearing at the same time if they can be fixed on just one peer.

Acknowledging alarms

Acknowledging all alarms (by selecting the alarms and clicking on the **Acknowledge** button) removes the Alarm icon from the web UI, but the alarms will still be listed on the **Alarms** page with a status of *Acknowledged*. If a new alarm occurs, the Alarm icon will reappear.

After any configuration changes to the TelePresence Conductor, or following a restart of the system, any *Acknowledged* alarms that are still unresolved will reappear with a status of *Raised*, and must be re-acknowledged.

Deleting alarms

You cannot delete alarms from the **Alarms** page. Alarms are removed by the TelePresence Conductor only after the required action or configuration change has been made.

Alarm information

The table below describes the fields that appear on the **Alarms** page.

Field	Description
Alarm	A description of the alarm.
State	**Raised**: a new alarm **Acknowledged**: the alarm is still in place but has been acknowledged by an administrator.
Severity	The severity of the condition that caused the alarm to be raised. Refer to Alarm severity for definitions.
Peer	If the TelePresence Conductor is part of a cluster, this indicates which peer the alarm relates to.
Action	How to resolve the situation that led to the alarm being raised. Where possible this will include a link to the page where any required configuration changes can be made.
ID	An identifier for the alarm. This can be provided to Cisco TAC engineers if required.

Alarm severity

The table below lists, in order of priority, each of the levels of severity that can be assigned to an alarm, and the definition of each.

Severity	Description
Emergency	A condition has occurred with the TelePresence Conductor hardware. Immediate action is required.
Alert	A condition has occurred with the TelePresence Conductor software. Immediate action is required.
Critical	The TelePresence Conductor has been configured in a way that will completely prevent it from working. Immediate action is required.
Error	A condition has occurred that will affect the performance of the TelePresence Conductor but it will continue to function to some extent.
Warning	A condition has occurred that may affect the performance of the TelePresence Conductor but it will continue to function to some extent.
Notice	A normal but significant condition has occurred. The TelePresence Conductor will continue to function normally.
Info	Information messages.
Debug	Information that Cisco TAC engineers may use for debugging.

Conference bridge status

The **Conference bridge status** page (**Status > Conference bridges**) shows all the conference bridges in your system's conference bridge pool, and their current status.

The information available includes:

Name	The name given to this conference bridge when it was added to the pool.
Description	The description given to this conference bridge when it was added to the pool.
Online/Offline	Indicates the current status of the conference bridge.
% capacity	Indicates the percentage of available ports currently in use.
Enabled/Disabled	Indicates whether the conference bridge has been administratively disabled or not.
Address:	The IP address or FQDN of the conference bridge.
Configure	Click **Configure** to go to the **Conference bridge pool** page where you can reconfigure the settings of this conference bridge.
Number of ports allocated	The number of ports that are currently in use or reserved for use.
Maximum number of ports on conference bridge	The total number of ports on the conference bridge.
Number of dedicated content ports allocated	The number of dedicated content ports that are currently in use.
Maximum number of dedicated content ports on conference bridge	The total number of dedicated content ports on the conference bridge.
Last unsuccessful contact attempt	For unusable conference bridges, this shows the local date and time that the TelePresence Conductor last attempted to contact the conference bridge.
Last active	For unusable conference bridges, this shows the local date and time that the conference bridge was last believed to be in a healthy state.

Conferences status

The **Conferences status** page (**Status > Conferences**) shows the number of conferences currently being managed by the TelePresence Conductor, and provides detailed information on each conference.

The information available includes:

Name	The name of the conference as it appears on the conference bridge.
State	Options are: ■ Connecting ■ Connected ■ Stopping ■ Stopped
Reserved auto-dialed chairperson ports	The number of ports that have been reserved for auto-dialed participants who have a role of Chairperson.
Used auto-dialed chairperson ports	The number of ports that are currently being used by auto-dialed participants who have a role of Chairperson.

Reserved ad hoc chairperson ports	The number of ports that have been reserved for participants (excluding any auto-dialed participants) who have a role of Chairperson.
Used ad hoc chairperson ports	The number of ports that are currently being used by participants (excluding any auto-dialed participants) who have a role of Chairperson.
Reserved cascade ports	The number of ports that have been reserved on the primary conference bridge for connections to additional conference bridges.
Used cascade ports	The number of ports that are currently being used by the primary conference bridge for connections to additional conference bridges.
Reserved auto-dialed ports	The number of ports that have been reserved for auto-dialed participants who have a role of Participant or Guest (i.e. not Chairperson).
Used auto-dialed ports	The number of ports that are currently being used by auto-dialed participants who have a role of Participant or Guest (i.e. not Chairperson).
Reserved ad hoc ports	For this release of the TelePresence Conductor, this will always be 0.
Used ad hoc ports	The number of ports that are currently being used by callers who have a role of Participant or Guest (i.e. not Chairperson) - this excludes any auto-dialed participants.
Primary conference bridge	The name (as it appears on the **Conference bridge pool** page) of the primary conference bridge, along with a breakdown of port usage on that particular conference bridge.
Cascade conference bridge	The name (as it appears on the **Conference bridge pool** page) of the cascade conference bridge, along with a breakdown of port usage on that particular conference bridge.
Conference created at	The date and time at which the conference was created.
Conference template	The template that was used for this conference.
Aliases which create/join this conference	The name (as it appears on the **Conference aliases** page) of each conference alias that was used to create or join the conference.
View the conference status on its own	Click this link to view the status for this conference only.
View the participants in this conference	Click this link to go to the Conference participants page, which provides information about all the participants in a particular conference.

Conference participants

The **Conference participants** page (**Status > Conferences**, then for a particular conference click **View the participants in this conference**) provides information about all the participants in a particular conference.

The information available includes:

Address	The registered alias (H.323 ID, E.164, SIP AOR) of the endpoint being used by the conference participant.

Protocol	Indicates whether the endpoint being used by the conference participant is using *SIP* or *H.323*.
State	*Connected*: this participant is currently connected to the conference *Disconnected*: this participant is no longer connected to the conference. *Dormant*: this indicates an auto-dialed participant that was unable to be dialed in to the conference.
Conference name	The name of the conference as it appears on the conference bridge. If the name is longer than 31 characters, a hash value will be displayed.
Join time	The local date and time at which this participant joined the conference.
Chairperson	*Yes*: this participant has a role of Chairperson. *No*: this participant has a role of Participant or Guest.
IP address	The IP address of the endpoint being used by the conference participant.
Conference bridge address	The address of the conference bridge (as it appears on the conference bridge pool page) of the conference bridge to which this participant is connected.
Call direction	*Incoming*: the participant joined the conference by dialing a conference alias. *Outgoing*: the participant was auto-dialed in to the conference by the conference bridge.

Event Log

About the Event Log

The TelePresence Conductor provides an event logging facility for troubleshooting and auditing purposes. This Event Log is a list of all the events that have occurred on your system since the last upgrade and records information about such things as conference creation and deletion, requests to join a conference, alarms raised, and conference bridge status changes. It may also contain system-level information.

The Event Log holds 22GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of event log data can be displayed through the web interface. The entire event log is included in a system snapshot.

The **Event Log** page (**Status > Event Log > All**) lets you view and search the Event Log.

The other sub-menus under the **Status > Event Log** menu provide you with a filtered view of the Event Log as follows:

- **Conference creation events** shows only those events relating to the creation of new conferences
- **Conference join events** shows only those events relating to users joining a conference
- **Conference destruction events** shows only those events relating to a conference being destroyed

Filtering the Event Log

The **Filter** area lets you view a subset of events based on words contained in the events.

By default, you can use the **Contains all of the words** field. Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: only includes events containing the exact phrase entered here.
- **Contains any of the words**: includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Note: you can use any combination of the above fields.

To reapply any modified filter conditions, click **Filter**.

To return to the complete Event Log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Reconfigure the log settings** takes you to the Logging configuration page. From this page, you can set up one or more remote servers to which the event log can be copied.

Viewing events

The **Results** area shows all the events matching all the current filter conditions, with the most recent being shown first.

Many events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after *Level*= filters the list to show only the events at that particular level.

Event Log color coding

Certain events in the Event Log are color-coded so that you can identify them more easily.

- **Green** indicates a successful event
- **Orange** acts as a warning, indicates an event about which you should be aware
- **Red** indicates a failure of some kind

Clustering

A Cisco TelePresence Conductor can be part of a cluster of up to three TelePresence Conductor systems.

This section covers the following topics:

About clusters

A TelePresence Conductor can be part of a cluster of up to three TelePresence Conductor systems. Each TelePresence Conductor in the cluster is a peer of every other TelePresence Conductor in the cluster. When a cluster has been created, any configuration changes made to one peer are shared immediately between all other peers in the cluster.

Clusters are used to provide redundancy in the rare case that a TelePresence Conductor becomes unavailable (for example, due to a network or power outage).

To avoid confusion, we recommend that you make all configuration changes on one peer. The only exception to this is any Peer-specific configuration.

For more information, refer to the *Cisco TelePresence Conductor Cluster Creation and Maintenance Deployment Guide*.

Peer IP addresses

CAUTION: never change the IP address of a TelePresence Conductor that is part of a cluster. see Changing a peer's IP address for more information.

Peers in a cluster are identified by IP address.

Cluster pre-shared key

The TelePresence Conductor uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer.

The **Cluster pre-shared key** is the common IPsec access key used by each peer to access every other peer in the cluster. This field is alphanumeric.

Each peer in the cluster must be configured with the same **Cluster pre-shared key**. This is a required field for peers in a cluster.

Note: a strong pre-shared key is important for system security and for the security of your video network.

Changing the pre-shared key

If you change the pre-shared key of one peer in the cluster, that peer will not be able to communicate with any other peers in the cluster that have a different pre-shared key. For this reason we recommend that if you must change the cluster's pre-shared key, you change it on all peers simultaneously.

Peer-specific configuration

Most items of configuration are applied to all peers in a cluster. However, the following items must be specified separately on each cluster peer.

Cluster configuration

The list of Peer IP addresses that make up the cluster has to be specified on each peer and they **must** be identical on each peer (the order in which they appear is not important).

The cluster pre-shared key has to be specified on each peer and **must** be identical for all peers.

Ethernet

The Ethernet speed is specific to each peer. Each peer may have slightly different requirements for the connection to their Ethernet switch.

IP

CAUTION: never change the IP address of a TelePresence Conductor that is part of a cluster.

The IPv4 address is specific to each peer. It **must** be different for each peer in the cluster.

The IPv4 subnet mask is specific to each peer. It can be different for each peer in the cluster.

The IPv4 gateway is specific to each peer. Each peer can use a different gateway.

Note: IP settings cannot be changed when the system is part of a cluster.

System host name and domain

The system host name is specific to each peer. We recommend that it is different for each peer in the cluster so that you can easily identify each system.

The DNS domain name is specific to each peer.

DNS servers

DNS servers are specific to each peer. Each peer can use a different set of DNS servers.

Time

The Configuring the NTP servers are specific to each peer. Each peer may use one or more different NTP servers.

The time zone is specific to each peer. Each peer may have a different local time.

SNMP

SNMP settings are specific to each peer. They can be different for each peer.

Logging

The Event Log on each peer will only report activity for the local TelePresence Conductor.

The list of remote syslog servers is specific to each peer. We recommend that you set up a remote syslog server to which the logs of all peers can be sent. This will allow you to have a global view of activity across all peers in the cluster. See the Logging configuration section for further details.

Security certificates

The Trusted CA Certificate and Server Certificate used by the TelePresence Conductor are specific to each peer. They must be uploaded individually on each peer.

Administration access

The SSH service and LCD panel settings are specific to each peer. They can be different for each peer.

Root account password

The password for the root account is specific to each peer. Each peer may have a different password, and for security reasons we recommend that they do.

Note: the username and password for the administrator account is shared across peers.

Creating a new cluster

To create a cluster, go to the **Clustering** page (**System > Clustering**).

This page lists the **IP address**es of all the peers in the cluster to which this TelePresence Conductor belongs. It also allows you to set the common **Cluster pre-shared key** used by each peer in the cluster to access all other peers. The **Status** section at the bottom of the page shows the current status of each peer.

Prerequisites

Before you create the cluster:

- Ensure that you can log in to the web UI of each TelePresence Conductor that is to be added to the cluster, and ensure that they each have the following settings configured as a minimum:
  - IPv4 address
  - IPv4 gateway
  - System host name (recommended so that you can easily differentiate between each peer in the cluster).
- Ensure that none of the systems to be clustered have any unresolved alarms.
- Ensure that all systems to be clustered have their time synchronized using an NTP server.
- **Note:** Deploying all peers in a cluster on the same LAN means they can be configured with the same

routing information such as local domain names and local domain subnet masks.

- We recommend that you create a backup of each system.

Placing the initial peer into cluster mode

1. Decide which peer is to be the initial peer. The configuration of this peer will be shared with all other peers as they are added to the cluster.
2. On this peer, go to the **Clustering** page (**System > Clustering**).
3. In the **Cluster pre-shared key** field, enter the common access key to be used by all peers when accessing each other.
4. In the **Peer 1 IP address** field, enter this peer's IP address.
5. **Save** this configuration.
6. Restart this peer (**Maintenance > Restart**, then click **Restart system**).

The initial peer will now be part of a "cluster" of one. The next step is to add each subsequent peer to the cluster.

Adding new peers to the cluster

After the initial peer has been placed into cluster mode, you can add up to two more peers to the cluster. Adding each additional peer is a two-step process:

1. Configuring the cluster to accept the new peer
2. Configuring the new peer to join the cluster

Note: any new peers added to the cluster must be in "standalone" mode. See Placing the peer in standalone mode for details.

Configuring the cluster to accept the new peer

On each existing cluster peer (i.e. the initial peer and any other peer that has already been added to the cluster):

1. Go to the **Clustering** page (**System > Clustering**).
2. In the next empty **Peer IP address** field, enter the new peer's IP address.
3. **Save** this configuration.

Configuring the new peer to join the cluster

1. On the new peer, go to the **Clustering** page (**System > Clustering**).
2. In the **Cluster pre-shared key** field, enter the common access key.
3. In the **Peer 1 IP address** field, enter the initial peer's IP address.
4. In the remaining **Peer IP address** fields, enter the IP addresses of all peers in the cluster, including the new peer.
5. **Save** this configuration.
6. Restart this peer (**Maintenance > Restart**, then click **Restart system**).

7. Log in to the new peer.

   Note: the new peer will now have the same Administrator username and password of the initial peer. You must use these credentials to log in.

The new peer will be added to the cluster, and its configuration will be updated to that of the cluster.

To add a third peer to the cluster, repeat the steps in Adding new peers to the cluster.

Updating the VCS's policy service

When you have created a cluster, you must ensure that the relevant policy service on the VCS is updated with details of all the peers in the cluster. See Server 1-3 address for more information.

Monitoring the status of the cluster

The status areas at the bottom of the **Clustering** page show you the current status of each peer in the cluster. To check that the cluster is not partitioned, make sure all peers have a status of *Up* on every peer.

Changing a peer's IP address

CAUTION: you must not change the IP address of a peer while it is part of a cluster.

If you want to change the IP address of a peer that is part of an existing cluster, you must perform the following steps, in order:

1. Remove the peer from the cluster. Refer to Removing a peer from an existing cluster for instructions.
2. Change the IP address of the peer (go to **System > IP** and change the entry in the **IPv4 address** field).
3. Re-add the peer to the cluster. Refer to Adding new peers to the cluster for instructions.

Removing a peer from an existing cluster

After a cluster has been set up you can remove individual peers from it. When a peer has been removed from the cluster, it will retain the configuration it had at the moment it was removed.

Note: if you want to remove **all** peers from a cluster, refer to Disbanding a cluster.

The instructions for removing a peer from a cluster differ depending on the current status of the peer - that is, whether it is live or out-of-service.

Removing a live peer from a cluster

Removing a live peer from a cluster is a two-step process:

1. Placing the peer in standalone mode
2. Removing the peer from the cluster

Each of these steps is described below.

Removing an out-of-service peer from a cluster

If one of the peers in a cluster has become 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 in Removing the peer from the cluster.

Note: if you want to place the out-of-service peer back into the cluster after successfully removing it, you must follow the instructions in Placing the peer in standalone mode and Adding new peers to the 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.

To do this:

1. On the peer to be removed, go to the **Clustering** page (**System > Clustering**).
2. Delete the **Cluster pre-shared key**.
3. Delete all entries from the **Peer IP address** fields.
4. **Save** this configuration.
5. Restart the peer (**Maintenance > Restart**, then click **Restart system**).
6. Delete all entries from the conference bridge pool.
7. Update the policy service on the VCS so that it does not include the removed peer. See Server 1-3 address for more information.

The peer will no longer consider itself part of the cluster. You must now follow the instructions in Removing the peer from the cluster.

Removing the peer from 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 cluster:

1. Go to the **Clustering** page (**System > Clustering**).
2. Delete the **Peer IP address** of the peer that has been removed from the cluster.
3. **Save** this configuration.
4. Repeat these steps for each remaining peer.

The removed peer will no longer be considered part of the cluster.

Disbanding a cluster

When a cluster is disbanded, all peers become standalone systems. They will retain the configuration they had at the moment the cluster was deleted.

Note: if you want to remove a single peer from a cluster without deleting the cluster, refer to Removing a peer from an existing cluster.

To delete a cluster, on each peer in the cluster:

1. Go to the **Clustering** page (**System > Clustering**).
2. Delete the **Cluster pre-shared key**.
3. Delete all entries from the **Peer IP address** fields.
4. **Save** this configuration.
5. Restart the peer (**Maintenance > Restart**, then click **Restart system**).
6. Repeat the above steps for every peer in the cluster.

Upgrading a cluster

When the software of one peer in a cluster is upgraded, that peer is unable to communicate with any other peers in the cluster that are not running the same software version. This means that any configuration changes made on one peer in the cluster will not be replicated to any other peers in the cluster that are running a different version of software.

In order to maintain the stability of the cluster, we recommend that:

- you upgrade each peer in the cluster one by one, waiting until the upgraded peer is back in service before upgrading the next peer
- you do not change any configuration on any peers in the cluster until all peers have been upgraded

For instructions on upgrading, refer to About upgrading software components.

Note: you should backup the system configuration of each peer before upgrading. For more information, refer to Cluster backup and restore.

Cluster backup and restore

The backup and restore process saves all configuration information for a particular TelePresence Conductor.

We recommend that you regularly backup all peers in the cluster. This ensures that peer-specific configuration information (see Peer-specific configuration) is saved and can be restored individually for each peer.

CAUTION: do not restore a backup made on one peer to another peer.

In all other aspects, the process for backing up and restoring peers in a cluster is the same as for standalone systems. For full instructions, refer to Backing up and restoring data.

About the maintenance menu

The options under the Maintenance menu allow you to perform the following tasks:

- Upgrade the TelePresence Conductor software
- Configure a remote syslog server
- Configure security certificates
- Backup and restore the TelePresence Conductor
- Create a system snapshot
- Configure incident reporting
- View or delete feedback receivers
- Restart, reboot and shutdown the TelePresence Conductor
- Access Developer resources

About upgrading software components

You can install new releases of the TelePresence Conductor software on your existing hardware. Software upgrades can be performed in one of two ways:

- Using the web interface - this is the recommended process.
- Using secure copy.

This guide describes how both of these methods are used to perform upgrades.

Note: you should read the section Before you upgrade prior to upgrading your software.

For information about upgrading peers in a cluster of TelePresence Conductors, refer to Upgrading a cluster.

Before you upgrade

Note:
- To avoid any performance degradation you are recommended to upgrade TelePresence Conductor components while the system is inactive.
- For specific information about upgrading peers in a cluster, see *Cisco TelePresence Conductor Cluster Creation and Maintenance Deployment Guide*.

Prerequisites

The upgrade requires you to have:

- a valid **Release key**, if you are upgrading to the next major release of the TelePresence Conductor (for example from XC1.0 to XC2.0). A release key is not required for dot releases (for example XC1.0 to XC1.1)
- a software image file for the component you want to upgrade, stored in a location that is locally accessible from your client computer
- release notes for the software version you are upgrading to — additional manual steps may be required

Contact your Cisco support representative for more information on obtaining these items.

Backing up before upgrading

You should backup your system configuration before upgrading. This can be done from the **Backup and restore** page (**Maintenance > Backup and restore**).

Installing and rebooting

Upgrading the TelePresence Conductor software is a two-stage process.

First, the new software image is uploaded onto the TelePresence Conductor. At the same time, the current configuration of the system is preserved, so that this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves rebooting the system. It is only during the reboot that the TelePresence Conductor installs the new software version and restores the previous configuration.

Rebooting will not affect existing conferences. However, if the TelePresence Conductor is not a part of a cluster, while the system is rebooting users will not be able to create new conferences, or join or rejoin existing conferences.

This two-stage process means that you can upload the new software to your system at any time, and then wait until a convenient moment to install the new version by rebooting the system.

Note: any configuration changes made between the software upload and the reboot will be lost when the system restarts using the new software version.

Upgrading using the web interface

The **Upgrade** page (**Maintenance > Upgrade**) is used to install newer versions of the TelePresence Conductor software.

Note:

- You should backup your system configuration before upgrading. Click **System backup** to go to the **Backup and restore** page.
- See Before you upgrade for full information about the upgrade process, prerequisites and how to backup your system.
- A system upgrade requires a system reboot to complete the process. Rebooting will not affect existing conferences. However, if the TelePresence Conductor is not a part of a cluster, while the system is rebooting users will not be able to create new conferences, or join or rejoin existing conferences.
- For additional information about upgrading peers in a cluster, see Upgrading a cluster.

To upgrade a component using the web interface:

1. Review the relevant release notes to see if any special steps are required either before or after installing the software image file.
2. Go to the **Upgrade** page (**Maintenance > Upgrade**).
3. Click **Browse** and select the software image file for the software version to which you want to upgrade.
4. Enter the **Release key** if required.
5. Click **Upgrade**.
   The TelePresence Conductor will start loading the file. This may take a few minutes.

6. When the **Upgrade confirmation** page is displayed, check that the expected **New software version** and **Release key** are displayed.
7. Check that the **MD5 hash** and **SHA1 hash** (if available) values displayed on the **Upgrade confirmation** page match the values displayed on the cisco.com page from where you have downloaded the software image file.
8. Click **Continue with upgrade**.
   The **System upgrade** page opens and displays a progress bar while the software installs.
9. When the software has uploaded, the page will display:
   ```
   Software successfully upgraded
   The system needs to be rebooted for the new software to take effect.
   ```
10. Click **Reboot system**.
    Note that if you made any configuration changes between uploading the software and rebooting, those changes will be lost when the system restarts.
    After the reboot is complete you are taken to the **Login** page.

The upgrade is now complete. The **Overview** and **Upgrade** pages now show the upgraded software component version numbers.

Upgrading using secure copy (SCP/PSCP)

To upgrade using a secure copy program such as SCP or PSCP (part of the PuTTY free Telnet/SSH package) you need to transfer two files to the TelePresence Conductor:

- A text file containing just the 16-character Release Key. Ensure there is no extraneous white space in this file.
- The file containing the software image.

To transfer these files:

1. Upload the Release Key file using SCP/PSCP to the **/tmp/** folder on the system. The target name must be **release-key**, for example:
   scp release-key root@10.0.0.1:/tmp/release-key.
2. Enter the root password when prompted.

   Note: the Release Key file must be uploaded before the image file.

3. Upload the software image using SCP/PSCP to the **/tmp** folder on the system. The target name must be **/tmp/tandberg-image.tar.gz**, for example:
   scp s42800xc11.tar.gz root@10.0.0.1:/tmp/tandberg-image.tar.gz
4. Enter the root password when prompted.
   The software installation begins automatically. Wait until the software has installed completely. This should not take more than five minutes.
5. Log in to the TelePresence Conductor and reboot the system. After about five minutes the TelePresence Conductor will be ready to use.

Note: if you make any further configuration changes before rebooting, those changes will be lost when the system restarts, so you are recommended to reboot your system immediately.

Logging configuration

The **Logging configuration** page (**Maintenance > Logging**) lets you enable remote logging by configuring up to four remote syslog servers to which copies of the TelePresence Conductor's Event Log are sent.

About the Event Log

The TelePresence Conductor provides an event logging facility for troubleshooting and auditing purposes. This Event Log is a list of all the events that have occurred on your system since the last upgrade and records information about such things as conference creation and deletion, requests to join a conference, alarms raised, and conference bridge status changes. It may also contain system-level information.

For more information see Event Log.

Remote logging of events

The Event Log is always stored locally on the TelePresence Conductor. However, it is often convenient to collect copies of all event logs from various systems in a single location. This is referred to as remote logging. This is particularly recommended for peers in a cluster.

To enable remote logging, configure the TelePresence Conductor with the IP address or Fully Qualified Domain Name (FQDN) of up to four **Remote syslog servers** to which the log will be written.

Note that:

- A computer running a BSD-style syslog server, as defined in *RFC 3164*, may be used as the remote log server.
- A TelePresence Conductor will not act as a remote log server for other systems.
- Events are always logged locally (to the Event Log) regardless of whether or not remote logging is enabled.
- If more than one remote syslog server has been configured, the same information will be sent to each.
- The TelePresence Conductor may use any of the 23 available syslog facilities for different messages. Specifically, LOCAL0..LOCAL7 (facilities 16..23) are used by different components of the application software on the TelePresence Conductor.

About the Tools menu

The **Tools** menu contains a number of features that can assist with troubleshooting of your system.

- Check pattern allows you to check whether a regular expression you intend to use when configuring a conference alias or auto-dialed participant on the TelePresence Conductor will have the expected result.
- Check dial plan allows you to check what will happen when a particular alias is received by the TelePresence Conductor.
- Diagnostic logging allows you to generate a diagnostic log of system activity over a period of time, and then to download the log so that it can be sent to your Cisco customer support representative.
- Ping allows you to check that a particular host system is contactable from the TelePresence Conductor and that your network is correctly configured to reach it.
- Traceroute allows you to discover the route taken by a network packet sent from the TelePresence Conductor to a particular destination host system.

- DNS lookup allows you to check which domain name server (DNS server) is responding to a request for a particular hostname.

Check pattern

The **Check pattern** tool (**Maintenance > Tools > Check pattern**) allows you to check whether a regular expression you intend to use when configuring a conference alias or auto-dialed participant on the TelePresence Conductor will have the expected result.

Note: for more information about regular expressions, see Regular expression reference.

When using this tool, what you must enter in each of the fields will depend on what the regular expression you are checking is being used for, as follows:

Field	Input	to check a conference alias...	to check an auto-dialed participant...
Pattern	The string to be checked.	enter the alias that is received by the TelePresence Conductor.	enter the name of the conference to which this auto-dialed participant is to be added.
Regular expression	The regular expression against which the **Pattern** will be compared.	enter the string configured in the **Incoming alias** field.	enter the string configured in the **Conference name match** field.
Replacement	The regular expression replacement string that defines how the **Pattern** will be modified if there is a match.	enter the string configured in the **Conference name** field.	enter the string configured in the **Address** field.

When you have completed the fields, click **Check pattern**. The results of the regular expression will appear, as follows:

Match result	States whether or not there was a successful match.
Replacement result	■ When checking a conference alias, this will be the resulting conference name. ■ When checking an auto-dialed participant, this will be the address that will be dialed by the TelePresence Conductor.

Note: when using this tool, a mock call will be placed to the TelePresence Conductor.

Check dial plan

The **Check dial plan** tool (**Maintenance > Tools > Check dial plan**) allows you to check what will happen when a particular alias is received by the TelePresence Conductor. It checks whether the incoming alias matches any of the configured conference aliases, and if so, what the resulting conference name will be and which role will be assigned to the caller when they join the conference.

To use this tool:

1. In the **Alias to check** field, enter the alias that you want to check, exactly as it will be received by the TelePresence Conductor.

2. Click **Check dial plan**.

A new section will appear showing the results of the check. If there was a match with a conference alias, the following information will be shown:

Successfully matched conference alias	The name of the conference alias that matched the alias being checked. The settings for this conference alias will be used by the TelePresence Conductor to determine how the call will be processed.
Resulting conference name	The name of the conference that will be created on the conference bridge when this alias is dialed.
Role	The role that will be assigned to a caller dialing in to the conference using this conference alias.
Incoming alias regular expression	The regular expression that was configured in the **Incoming alias** field of the matching conference alias.
Conference name replacement string	The replacement string that was configured in the **Conference name** field of the matching conference alias.

Diagnostic logging

The **Diagnostic logging** tool (**Maintenance > Tools > Diagnostic logging**) can be used to assist in troubleshooting system issues.

It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log so that it can be sent to your Cisco customer support representative.

To use this tool:

1. Go to the **Diagnostic logging** page.
2. Click **Start new log**.
3. (Optional) Enter some **Marker** text and click **Add marker**.
   - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
   - You can add as many markers as required, at any time while the diagnostic logging is in progress.
   - Marker text is added to the log with a "`DEBUG_MARKER`" tag.
4. Reproduce the system issue you want to trace in the diagnostic log.
5. Click **Stop logging**.
6. Click **Download log** to save the diagnostic log to your local file system. You are prompted to save the file (the exact wording depends on your browser).
7. Send the downloaded diagnostic log file to your Cisco support representative, if you have been requested to do so.

Note that:

- Only one diagnostic log can be produced at a time; creating a new diagnostic log will replace any previously produced log.
- The TelePresence Conductor continually logs all system activity to a unified log file. The diagnostic logging facility works by extracting a portion of this unified log. On busy systems the unified log file may become full over time and will discard historic log data so that it can continue logging current activity. This means that all or part of your diagnostic log could be overwritten. The system will warn you if you attempt to download a partial diagnostic log file.
- The diagnostic log will continue logging all system activity until it is stopped, including over multiple login sessions and system restarts.

Clustered systems

Diagnostic logging can also be used if your TelePresence Conductor is a part of a cluster, however some activities only apply to the "current" peer (the peer to which you are currently logged in to as an administrator):

- Each cluster peer maintains its own unified log, and logs activity that occurs only on that peer.
- The start and stop logging operations are applied to every peer in the cluster, regardless of the current peer.
- Marker text is only applied to log of the current peer.
- You can only download the diagnostic log from the current peer.
- To add markers to other peers' logs, or to download diagnostic logs from other peers, you must log in as an administrator to that other peer.

Ping

The **Ping** tool (**Maintenance > Tools > Network utilities > Ping**) can be used to assist in troubleshooting system issues.

It allows you to check that a particular host system is contactable and that your network is correctly configured to reach it. It reports details of the time taken for a message to be sent from the TelePresence Conductor to the destination host system.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system you want to contact.
2. Click **Ping**.

A new section will appear showing the results of the contact attempt. If successful, it will display the following information:

Host	The hostname and IP address returned by the host system that was queried.
Response time (ms)	The time taken (in ms) for the request to be sent from the TelePresence Conductor to the host system and back again.

Traceroute

The **Traceroute** tool (**Maintenance > Tools > Network utilities > Traceroute**) can be used to assist in troubleshooting system issues.

It allows you to discover the route taken by a network packet sent from the TelePresence Conductor to a particular destination host system. It reports the details of each router along the path, and the time taken for each router to respond to the request.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host that you want to trace the route to.
2. Click **Traceroute**.

A new section will appear with a banner stating the results of the trace, and showing the following information for each router in the path:

TTL	(Time to Live). This is the hop count of the request, showing the sequential number the router.
Response	This shows the IP address of the router, and the time taken (in ms) to respond to each packet received from the TelePresence Conductor. *** indicates that the router did not respond to the request.

The route taken between the TelePresence Conductor and a particular host may vary for each Traceroute request.

DNS lookup

The **DNS lookup** tool (**Maintenance > Tools > Network utilities > DNS lookup**) can be used to assist in troubleshooting system issues.

It allows you to check which domain name server (DNS server) is responding to a request for a particular hostname.

To use this tool:

1. In the **Host** field, enter either:
   - the name of the host you want to query, or
   - an IPv4 or IPv6 address if you want to perform a reverse DNS lookup
2. In the **Query type** field, select the type of record you want to search for:
   (for reverse lookups the **Query type** is ignored - the search automatically looks for PTR records)

Option	Searches for...
All	any type of record
A (IPv4 address)	a record that maps the hostname to the host's IPv4 address
AAAA (IPv6 address)	a record that maps the hostname to the host's IPv6 address
SRV (SIP and H.323 servers)	SRV records (which includes those specific to either H.323 or SIP servers, see below).
NAPTR (Name authority pointer)	a record that rewrites a domain name (into a URI or other domain name for example).

3. Click **Lookup**.

A separate DNS query is performed for each selected **Query type**. The domain that is included within the query sent to DNS depends upon whether the supplied **Host** is fully qualified or not (a fully qualified host name contains at least one "dot"):

- If the supplied **Host** is fully qualified:
  - DNS is queried first for **Host**
  - If the lookup for **Host** fails, then an additional query for **Host.<system_domain>** is performed (where **<system_domain>** is the **Domain name** as configured on the **DNS** page)
- If the supplied **Host** is not fully qualified:
  - DNS is queried first for **Host.<system_domain>**
  - If the lookup for **Host.<system_domain>** fails, then an additional query for **Host** is performed

For SRV record type lookups, multiple DNS queries are performed as follows:

- An SRV query is made for each of the following _service._protocol combinations:
  - _h323ls._udp.<domain>
  - _h323cs._tcp.<domain>
  - _sips._tcp.<domain>
  - _sip._tcp.<domain>
  - _sip._udp.<domain>
    In each case, as for all other query types, either one or two queries may be performed for a <domain> of either **Host** and/or **Host.<system_domain>**.

Results

A new section will appear showing the results of all of the queries. If successful, it will display the following information:

Query type	The type of query that was sent by the TelePresence Conductor.
Name	The hostname contained in the response to the query.
TTL	The length of time (in seconds) that the results of this query will be cached by the TelePresence Conductor.
Class	**IN** (internet) indicates that the response was a DNS record involving an internet hostname, server or IP address.
Type	The record type contained in the response to the query.
Response	The content of the record received in response to the query for this **Name** and **Type**.

Example

If the system's **Domain name** is set to **example.com**, a lookup for a **Host** of **host_name** with a **Query type** of *All* would result in the following DNS queries:

```
A     host_name.example.com
AAAA  host_name.example.com
NAPTR host_name.example.com
SRV   host_name.example.com
SRV   _h323ls._udp.host_name.example.com
SRV   _h323cs._tcp.host_name.example.com
SRV   _sips._tcp.host_name.example.com
SRV   _sip._tcp.host_name.example.com
SRV   _sip._udp.host_name.example.com
```

In each of these cases, if the query is unsuccessful an additional query would be made for **host_name** only.

Trusted CA Certificate

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

- To upload a new file of CA certificates, **Browse** to the required PEM file and click **Upload CA certificate**. This will replace any previously uploaded CA certificates.
- To replace the currently uploaded file with a default list of trusted CA certificates, click **Reset to default CA certificate**.
- To view the currently uploaded file, click **Show CA certificate**.

Server Certificate

The **Server Certificate** page (**Maintenance > Security certificates> Server Certificate**) allows you to upload the TelePresence Conductor's server certificate. This certificate is used to identify the TelePresence Conductor when it communicates with client systems using TLS encryption, and with web browsers over HTTPS.

- To upload a server certificate, use the **Browse** buttons to select the **server certificate** PEM file and the **server private key** PEM file that is used to encrypt it. After selecting both files, click **Upload server certificate data**. Note that the private key must not be password protected.
- To replace the currently uploaded server certificate with the TelePresence Conductor's default certificate, click **Reset to default server certificate**.
- To view the currently uploaded server certificate file, click **Show server certificate**.

Backing up and restoring data

This section provides information on backing up and restoring TelePresence Conductor data.

Backing up and restoring overview gives information about when to create a backup, the contents of the backup file, and limitations you should be aware of.

Creating a backup describes how to backup TelePresence Conductor data.

Restoring a previous backup describes how to restore TelePresence Conductor data.

For extra information about backing up and restoring peers in a cluster, refer to the Cluster backup and restore section.

Backing up and restoring overview

The **Backup and restore** page (**Maintenance > Backup and restore**) is used to create and restore backup files of your TelePresence Conductor data.

When to create a backup

You are recommended to create a backup in the following situations:

- before performing an upgrade
- before performing a system restore
- in demonstration and test environments if you want to be able to restore the TelePresence Conductor to a known configuration after significant configuration changes have been made

Content of the backup file

The data in the backup includes:

- system configuration settings
- clustering configuration
- security certificates
- administrator account details

Event Logs are not included in the backup files.

Limitations

- Backups can only be restored to a TelePresence Conductor running the same version of software from which the backup was made.
- You can create a backup on one TelePresence Conductor and restore it to a different TelePresence Conductor, for example if the original system has failed. If you attempt to restore a backup made on a different TelePresence Conductor, you will receive a warning message, but you will be allowed to continue.
- Backups should not be used to copy data between TelePresence Conductor units.

Note: you are recommended to take the TelePresence Conductor unit out of service before performing a restore.

For extra information about backing up and restoring peers in a cluster, refer to the Cluster backup and restore section.

Creating a backup

To create a backup of the TelePresence Conductor's data:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. Click **Create system backup file**.
3. 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: **<hardware serial number>_<date>_<time>_backup.tar.gz**.
4. Save the file to a designated location.

Note: backups contain security sensitive information. You should ensure that you handle and store them carefully in such a way as to prevent unauthorized access.

Restoring a previous backup

To restore the TelePresence Conductor to a previous configuration of data:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. In the **Restore** section, **Browse** to the backup file containing the configuration you want to restore.
3. Click **Upload system backup file**.
4. The TelePresence Conductor checks the file and takes you to the **Restore confirmation** page.
   - If the backup file is not valid, you will receive an error message at the top of the **Backup and restore** page.

   You are shown the current software version and hardware serial number.
5. Read all the warning messages that appear before proceeding with the restore.
6. Click **Continue with system restore** to continue with the restore process. This will restart your system.

- Click **Abort system restore** if you need to exit the restore process and return to the **Backup and restore** page.

After the system restarts, you are taken to the login page.

Creating a system snapshot

The **System snapshot** page (**Maintenance > System snapshot**) lets you create files that can be used for diagnostic purposes. The files should be sent to your support representative at their request to assist them in troubleshooting issues you may be experiencing.

You can create several types of snapshot file:

- **Status snapshot**: contains the system's current configuration and status settings.
- **Logs snapshot**: contains log file information (including the Event Log, Configuration Log and Network Log).
- **Full snapshot**: contains a complete download of all system information. The preparation of this snapshot file may take several minutes to complete and may lead to a drop in system performance while the snapshot is in progress.

To create a system snapshot file:

1. Click one of the snapshot buttons to start the download of the snapshot file. Typically your support representative will tell you which type of snapshot file is required.
   - The snapshot creation process will start. This process runs in the background. If required, you can navigate away from the snapshot page and return to it later to download the generated snapshot file.
   - When the snapshot file has been created, a **Download snapshot** button will appear.
2. Click **Download snapshot**. A pop-up window appears and prompts you to save the file (the exact wording depends on your browser). Select a location from where you can easily send the file to your support representative.

Note: system snapshots contain security sensitive information. You should ensure that you handle and store them carefully in such a way as to prevent unauthorized access.

Incident reporting

The incident reporting feature of the TelePresence Conductor automatically saves information about critical system issues such as application failures. You can:

- configure the TelePresence Conductor to send the reports automatically to Cisco customer support
- view the reports from the TelePresence Conductor web interface
- download and send the reports manually to Cisco (usually at the request of Cisco customer support)

The information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures. All information gathered during this process will be held in confidence and used by Cisco personnel for the sole purpose of issue diagnosis and problem resolution.

This feature is only intended for use at the request of Cisco customer support in exceptional situations, and is *Off* by default.

Incident reporting warning: privacy-protected personal data

IN NO EVENT SHOULD PRIVACY-PROTECTED PERSONAL DATA BE INCLUDED IN ANY REPORTS TO CISCO.

Privacy-Protected Personal Data means any information about persons or entities that the Customer receives or derives in any manner from any source that contains any personal information about prospective, former, and existing customers, employees or any other person or entity. Privacy-Protected Personal Data includes, without limitation, names, addresses, telephone numbers, electronic addresses, social security numbers, credit card numbers, customer proprietary network information (as defined under 47 U.S.C. § 222 and its implementing regulations), IP addresses or other handset identifiers, account information, credit information, demographic information, and any other information that, either alone or in combination with other data, could provide information specific to a particular person.

PLEASE BE SURE THAT PRIVACY-PROTECTED PERSONAL DATA IS NOT SENT TO CISCO WHEN THE TELEPRESENCE CONDUCTOR IS CONFIGURED TO AUTOMATICALLY SEND REPORTS.

IF DISCLOSURE OF SUCH INFORMATION CANNOT BE PREVENTED, PLEASE DO NOT USE THE AUTOMATIC CONFIGURATION FEATURE. Instead, copy the data from the Incident detail page and paste it into a text file. You can then edit out any sensitive information before forwarding the file on to Cisco customer support.

Incident reports will always be saved locally, and can be viewed via the Incident view page.

Sending incident reports automatically

Please read the privacy-protected personal data warning before you decide whether to enable automatic incident reporting.

To configure the TelePresence Conductor to send incident reports automatically to Cisco customer support:

1. Go to the **Incident reporting configuration** page (**Maintenance > Incident reporting > Configuration**).
2. Set the **Incident reports sending mode** to *On*.
3. Specify the **Incident reports URL** of the web service to which any error reports are to be sent. The default is `https://cc-reports.cisco.com/submitapplicationerror/`.

Note that if the **Incident reports sending mode** is *Off*, incidents will not be sent to any URL but they will still be saved locally and can be viewed and downloaded from the **Incident detail** page.

Sending incident reports manually

Please read the privacy-protected personal data warning before you decide whether to send an incident report manually to Cisco.

To send an incident report manually to Cisco customer support:

1. Go to the **Incident view** page (**Maintenance > Incident reporting > View**).
2. Click on the incident you want to send. You will be taken to the **Incident detail** page.
3. Scroll down to the bottom of the page and click **Download incident report**. You will be given the option to save the file.
4. Save the file in a location from where it can be forwarded to Cisco customer support.

Removing sensitive information from a report

The details in the downloaded incident report are Base64-encoded, so you will not be able to meaningfully view or edit the information within the file.

If you need to edit the report before sending it to Cisco (for example, if you need to remove any potentially sensitive information) you must copy and paste the information from the **Incident detail** page into a text file, and edit the information in that file before sending it to Cisco.

Viewing incident reports

The **Incident view** page (**Maintenance > Incident reporting > View**) shows a list of all incident reports that have occurred since the TelePresence Conductor was last upgraded. A report is generated for each incident, and the information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures.

For each report the following information is shown:

Field	Description
Time	The date and time when the incident occurred.
Version	The TelePresence Conductor software version running when the incident occurred.
Build	The internal build number of the TelePresence Conductor software version running when the incident occurred.
State	The current state of the incident: *Pending*: indicates that the incident has been saved locally but not sent. *Sent*: indicates that details of the incident have been sent to the URL specified in the Incident reporting configuration page.

To view the information contained in a particular incident report, click on the report's *Time*. You will be taken to the Incident detail page, from where you can view the report on screen, or download it as an XML file for forwarding manually to Cisco customer support.

Incident report details

The **Incident detail** page (**Maintenance > Incident reporting > View**, then click on a report's *Time*) shows the information contained in a particular incident report.

This is the information that is sent to the external web service if you have enabled **Incident reports sending mode** (via **Maintenance > Incident reporting > Configuration**). It is also the same information that is downloaded as a Base64-encoded XML file if you click **Download incident report**.

The information contained in the report is:

Field	Description
Time	The date and time when the incident occurred.
Version	The TelePresence Conductor software version running when the incident occurred.
Build	The internal build number of the TelePresence Conductor software version running when the incident occurred.
Name	The name of the software.
System	The system name (if configured), otherwise the IP address.
Serial number	The hardware serial number.
Process ID	The process ID the TelePresence Conductor application had when the incident occurred.
Release	A true/false flag indicating if this is release build (rather than a development build).
User name	The name of the person that built this software. This is blank for release builds.
Stack	The trace of the thread of execution that caused the incident.
Debug information	A full trace of the application call stack for all threads and the values of the registers. **CAUTION:** for each call stack, the Debug information includes the contents of variables which may contain some sensitive information, for example alias values and IP addresses. If your deployment is such that this information could contain information specific to a particular person, please read the warning regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

View or delete feedback receivers

TelePresence Conductor offers a feedback interface, which TMS and Prime Collaboration Manager (PCM) use to register for feedback about the current state of the TelePresence Conductor.

Whenever TMS or PCM register for feedback from TelePresence Conductor an entry for the TMS's or PCM's IP address is added to the TelePresence Conductor's database. The TelePresence Conductor will attempt to connect to the configured IP address(es) whenever there is an event, even if the IP address is not reachable anymore.

To view or delete defunct feedback receivers go to the **Feedback receivers** page (**Maintenance > Feedback receivers**). When deleting one or more feedback receiver, select the feedback receiver(s) and click **Delete**.

Restarting

The **Restart** page (**Maintenance > Restart**) allows you to restart the TelePresence Conductor without having physical access to the hardware.

CAUTION: do not restart the TelePresence Conductor while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your Cisco customer support representative.

The restart function shuts down and restarts the TelePresence Conductor application software, but not the operating system or hardware. Some configuration changes require a restart of the TelePresence Conductor before they take effect. A **Restart** button is at the bottom of most web pages that include such settings, and clicking it takes you to the **Restart** page. A system alarm will remain in place until the system is restarted.

Note that:

- Restarting will not affect existing conferences; these will be left running.
- If the TelePresence Conductor is not a part of a cluster, while the system is restarting users will not be able to create new conferences, or join or rejoin existing conferences.
- If the TelePresence Conductor is part of a cluster, restarting the system will not affect users' ability to create, join or rejoin conferences.

Restarting using the web interface

To restart the TelePresence Conductor using the web interface:

1. Go to **Maintenance > Restart**, or from a relevant configuration page, click the **Restart** button. You are taken to the **Restart** page.
2. Click **Restart system**.
   The **Restarting** page appears, with an orange bar indicating progress.

Note: if after a restart or reboot you see a message saying "Cannot connect because the TelePresence Conductor web server is not responding", wait 10 seconds or so before refreshing the page.

After the system has successfully restarted, you are automatically taken to the **Login** page.

Note: to shut down and restart the TelePresence Conductor operating system and hardware in addition to the TelePresence Conductor application software, choose the Reboot function (**Maintenance > Reboot**). Restarting is quicker than rebooting.

Rebooting

The **Reboot** page (**Maintenance > Reboot**) allows you to reboot the TelePresence Conductor without having physical access to the hardware.

CAUTION: do not reboot the TelePresence Conductor while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your Cisco customer support representative.

The reboot function shuts down and restarts the TelePresence Conductor application software, operating system and hardware. Reboots are normally only required after software upgrades and are performed as part of the upgrade process.

Note that:

- Rebooting will not affect existing conferences; these will be left running.
- If the TelePresence Conductor is not a part of a cluster, while the system is rebooting users will not be able to create new conferences, or join or rejoin existing conferences.

- If the TelePresence Conductor is part of a cluster, rebooting the system will not affect users' ability to create, join or rejoin conferences.

Rebooting using the web interface

To reboot the TelePresence Conductor using the web interface:

1. Go to **Maintenance > Reboot**. You are taken to the **Reboot** page.
2. Click **Reboot system**.
   The **Rebooting** page appears, with an orange bar indicating progress.

Note: if after a restart or reboot you see a message saying "Cannot connect because the TelePresence Conductor web server is not responding", wait 10 seconds or so before refreshing the page.

After the system has successfully rebooted, you are automatically taken to the **Login** page.

Note: to shut down and restart the TelePresence Conductor application software but not the operating system and hardware, choose the restart function (**Maintenance > Restart**). Restarting is quicker than rebooting, but you may want to perform a reboot if a restart has not had the desired effect.

Shutting down

The **Shutdown** page (**Maintenance > Shutdown**) allows you to turn off the TelePresence Conductor without having physical access to the hardware.

CAUTION: do not shut down the TelePresence Conductor while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your Cisco customer support representative.

The system must be shut down before it is unplugged. Avoid uncontrolled shutdowns, in particular the removal of power to the system during normal operation.

After the system has been shut down, the only way it can be restarted (unless it is a virtual appliance) is by pressing the soft power button on the unit itself. You must therefore have physical access to the unit if you want to restart it after it has been shut down.

Note that:

- Shutting down the system will not affect existing conferences; these will be left running.
- If the TelePresence Conductor is not a part of a cluster, after the system has shut down, users will not be able to create new conferences, or join or rejoin existing conferences.
- If the TelePresence Conductor is part of a cluster, shutting down the system will not affect users' ability to create, join or rejoin conferences.

Shutting down using the web interface

To shut down the TelePresence Conductor:

1. Go to **Maintenance > Shutdown**. You are taken to the **Shutdown** page.
2. Click **Shutdown system**.
   The **Shutting down** page appears. This page remains in place after the system has successfully shut down but any attempts to refresh the page or access the TelePresence Conductor will be unsuccessful.

Developer resources

The TelePresence Conductor includes some features that are intended for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

WARNING: incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

These features are:

- Debugging and system administration tools
- Experimental menu

Debugging and system administration tools

WARNING: these features are not intended for customer use unless on the advice of a Cisco support representative. Incorrect usage of these features could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

The TelePresence Conductor includes a number of debugging and system admin tools that allow administrators to inspect what is happening at a detailed level on a live system, including accessing and modifying configuration data and accessing network traffic.

To access these tools:

1. Open an SSH session.
2. Log in as root.
3. Follow the instructions provided by your Cisco support representative.

Experimental menu

The TelePresence Conductor web interface contains a number of pages that are not intended for use by customers. These pages exist for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

WARNING: incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

To access these pages:

1. Go to `https://<TelePresence Conductor host name or IP address>/setaccess`
   The **Set access** page appears.
2. In the **Access password** field, enter `qwertsys`.
3. Click **Enable access**.

A new top-level **Experimental** menu will appear to the right of the existing menu items.

Reference

This section provides supplementary information regarding the administration of the TelePresence Conductor, including:

Regular expression reference

This section provides the following information about regular expressions:

- About regular expressions provides a table of common regular expressions.
- Regular expression examples - conference aliases shows how to use regular expressions to achieve some basic functions such as prefix and suffix matching, stripping, and replacing. These can be used when configuring conference aliases for either meetings or lectures.
- Regular expression examples - lectures builds on the examples already given to show how to use regular expressions when configuring conference aliases for lectures.
- Regular expression examples - auto-dialed participants shows how to use regular expressions to match a range of conference names and convert each into an address to be dialed.

Note: the **Check pattern** page (**Maintenance > Tools >Check pattern**) allows you to check whether a regular expression you intend to use when configuring a conference alias or auto-dialed participant on the TelePresence Conductor will have the expected result.

About regular expressions

Regular expressions can be used when Creating and editing conference aliases and when Creating and editing auto-dialed participants.

With conference aliases, regular expressions can be used to specify a pattern for the **Incoming alias**, and a replace string can then be used to specify the way in which any alias that matches that pattern is transformed to create the **Conference name**.

With auto-dialed participants, regular expressions can be used to specify a pattern for the **Conference name match**, and a replace string can then be used to specify the way in which any conference name that matches that pattern is transformed to create the **Address**.

The TelePresence Conductor uses POSIX format regular expression syntax. The table below provides a list of some commonly used special characters in regular expression syntax. This is only a subset of the full range of expressions available. For a detailed description of regular expression syntax see the publication *Regular Expression Pocket Reference*.

On the TelePresence Conductor, regular expressions are compared with the string being matched as a whole line. If the string includes other characters that follow after the matched characters, this will not be considered a match. For example, **`meet.ben`** will match **`meet.ben`** but not **`meet.benjamin`**.

For examples of regular expression usage with the TelePresence Conductor, see:

- Regular expression examples - conference aliases
- Regular expression examples - lectures
- Regular expression examples - auto-dialed participants

Common regular expressions

Character	Description	Example
`.`	Matches any single character.	
`*`	Matches 0 or more repetitions of the previous match.	`.*` will match against an empty string or any sequence of characters.
`+`	Matches 1 or more repetitions of the previous match.	`.+` will match against any sequence of characters.
`?`	Matches 0 or 1 repetition of the previous match.	`meet.alice(@example\.com)?` will match either `meet.alice` or `meet.alice@example.com`
`\`	Escapes a regular expression special character.	`\.` will match against a full stop (i.e. `.`) only.
`\d`	Matches any decimal digit, i.e. 0-9.	`\d\d\d` will match any number that is 3 digits long.
`[...]`	Matches a set of characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the `-` character and then the last character in the range. You cannot use special characters within the `[]` - they will be taken literally.	`[a-z]` will match against any lower case alphabetical character. `[a-zA-Z]` will match against any alphabetical character. `[0-9#*]` will match against any single E.164 character - the E.164 character set is made up of the digits 0-9 plus the hash key (#) and the asterisk key (*).
`(...)`	Groups a set of matching characters together. Groups can then be referenced in order using the characters `\1`, `\2`, etc. as part of a replace string.	A regular expression can be constructed to transform a URI containing a user's full name to a URI based on their initials. The regular expression `(.).*_(.).*(@example.com)` would match against the user `john_smith@example.com` and with a replace string of `\1\2\3` would transform it to `js@example.com`.
`|`	Matches against one expression or an alternate expression.	`.*@example.(net|com)` will match against any URI for the domain `example.com` or the domain `example.net`.
`^`	Signifies the start of a line. When used immediately after an opening brace, negates the character set inside the brace.	`^meet.*` will match `meet.alice` but not `alice.meeting` `[^abc]` matches any single character that is NOT one of a, b or c.
`(?!...)`	Negative lookahead. Defines a subexpression that must not be present in order for there to be a match.	`(?!.*@example.com$).*` will match any string that does not end with `@example.com`. `(?!alice).*` matches any string that does not start with `alice`.
`(?<!...)`	Negative lookbehind. Defines a subexpression that must not be present in order for there to be a match.	`.*(?<!net)` matches any string that does not end with `net`.

Regular expression examples - conference aliases

When configuring a conference alias, you can use a regular expression (regex) in the **Incoming alias** field in combination with a replace string in the **Conference name** fields. This allows you to use advanced pattern matching and replacing functions of regular expressions.

The examples below show how to use regular expressions to achieve some basic functions such as prefix and suffix matching, stripping, and replacing. These can be used when configuring conference aliases for either meetings or lectures.

For specific examples of using regular expressions when configuring conference aliases for lectures, see Regular expression examples - lectures.

The **Check pattern** page (**Maintenance > Tools >Check pattern**) allows you to check whether a regular expression you intend to use when configuring a conference alias or auto-dialed participant on the TelePresence Conductor will have the expected result.

Note: when configuring conference aliases for lectures, you **must** ensure that the Conference name for the Chairperson alias and the Guest alias resolve to the same string. If you do not, they will end up in separate conferences.

Matching a prefix

To allow users to create a conference by dialing a given prefix followed by a string, and use exactly what they dialed as the conference name:

	Incoming alias	Conference name
regex	`(meet\..+)`	`\1`
example	meet.alice	meet.alice

Stripping a prefix

To allow users to create a conference by dialing a given prefix followed by a string, and use what they dialed minus the prefix as the conference name:

	Incoming alias	Conference name
regex	`meet\.(.+)`	`\1`
example	meet.alice	alice

Replacing a prefix

To allow users to create a conference by dialing a given prefix followed by a string, and replace the prefix they dialed with another string to create the conference name:

	Incoming alias	Conference name
regex	`meet\.(.*)`	`666\1`
example	meet.alice	666alice

Matching a suffix

To allow users to create a conference by dialing a string followed by a given suffix, and use exactly what they dialed as the conference name:

	Incoming alias	Conference name
regex	`(.*\.meet)`	`\1`
example	alice.meet	alice.meet

Stripping a suffix

To allow users to create a conference by dialing a string followed by a given suffix, and use what they dialed minus the suffix as the conference name:

	Incoming alias	Conference name
regex	`(.*)\.meet`	`\1`
example	alice.meet	alice

Replacing a suffix

To allow users to create a conference by dialing a string followed by a given suffix, and replace the suffix they dialed with another string to create the conference name:

	Incoming alias	Conference name
regex	`(.*)\.meet`	`\1.meeting`
example	alice.meet	alice.meeting

Adding a prefix or suffix

To allow users to create a conference by dialing a given string, and add another string before or after what they dialed to create the conference name:

	Incoming alias	Conference name
regex	`(meet)\.(.*)`	`conference.\1.\2`
example	meet.alice	conference.meet.alice
regex	`(meet)\.(.*)`	`\1.\2.conference`
example	meet.alice	meet.alice.conference

Matching an alias with or without a domain appended

To allow users to dial the same conference alias from either an H.323 endpoint (which will not append its domain) or a SIP endpoint (which will append its domain):

	Incoming alias	Conference name
regex	`meet\.([^@]*)(@example\.com)?`	`meet.\1`
example	meet.alice@example.com	meet.alice
example	meet.alice	meet.alice

Regular expression examples - lectures

When configuring a conference alias for lectures, you can use a regular expression (regex) in the **Incoming alias** field in combination with a replace string in the **Conference name** field for both the Chairperson and Guest aliases. The conference name for both chairperson and guest have to be the same. Using the **Incoming alias** field allows you to apply advanced pattern matching and replacing functions of regular expressions.

The examples on this page build on the examples given in Regular expression examples - conference aliases, which show how to use regex to achieve some basic functions such as prefix and suffix matching, stripping, and replacing. These can be used when configuring conference aliases for either meetings or lectures.

The **Check pattern** page (**Maintenance > Tools >Check pattern**) allows you to check whether a regular expression you intend to use when configuring a conference alias or auto-dialed participant on the TelePresence Conductor will have the expected result.

Note: when configuring conference aliases for lectures, you **must** ensure that the Conference name for the Chairperson alias and the Guest alias resolve to the same string. If you do not, they will end up in separate conferences.

Stripping a prefix

One of the simplest ways to use regex when configuring conference aliases for lectures is to allocate different prefixes to the Chairperson and Guest conference aliases, and then strip the prefix to result in the conference name. Below is an example of how to do this, using regular expressions:

	Incoming alias	Conference name
Chairperson regex	`show\.(.*)`	`\1`
example	show.sales.team	sales.team
Guest regex	`watch\.(.*)`	`\1`
example	watch.sales.team	sales.team

Regular expression examples - auto-dialed participants

When configuring an auto-dialed participant, you can use a regular expression (regex) in the **Conference name match** in combination with a replace string in the **Address** field. This allows you to use wildcards and other advanced pattern matching and replacing functions of regular expressions to match a range of conference names and convert each into an address to be dialed.

The examples below show how to use regular expressions to achieve some basic functions such as matching a conference name, and adding and replacing prefixes.

The **Check pattern** page (**Maintenance > Tools >Check pattern**) allows you to check whether a regular expression you intend to use when configuring a conference alias or auto-dialed participant on the TelePresence Conductor will have the expected result.

Note: if you have used regular expressions when creating conference aliases, the conference names that are being generated will vary depending on the incoming alias. You must therefore ensure that any regex you use to match against potential conference names will cover all possible outcomes of the regex that was used to generate the conference name.

Adding a prefix to all conference names

In this example we want to record all conferences. Our dial plan is set up so that any calls to addresses that start with **`record.`** are routed to our Cisco TelePresence Content Server recording device.

We create an auto-dialed participant that matches any conference name and adds the prefix **`record.`** as follows:

Field	Input	Explanation	Example
Conference name match	(.*)	This regex is the default for this field. It will match against all possible conference names. This will result in the **Address** always being dialed for any conferences created using the specified **Conference template**.	sales_ meeting
Address	record.\1	This replace string will result in the conference name being prefixed with **`record.`** to create the address to be dialed.	record.sales_ meeting

Matching a prefix

In this example, we want to record all **all hands** conferences.

Our dial plan is set up so that:

- these conferences all begin with **allhands.**, for example **allhands.sales** and **allhands.operations**.
- any calls to addresses that start with **`record.`** are routed to our Cisco TelePresence Content Server recording device.

We set up an auto-dialed participant that matches any conference name that starts with **allhands**, and replaces that prefix with **`record.`** as follows:

Field	Input	Explanation	Example
Conference name match	allhands\.(.*)	This regex will match against any conference names beginning with **`allhands.`**.	allhands.sales
Address	record.\1	This replace string will result in **`allhands.`** being removed from the conference name and replaced with **`record.`** to create the address to be dialed.	record.sales

Combining the use of regular expressions in conference aliases and auto-dialed participants

The following example shows how you can combine the use of regular expressions when creating conference aliases and auto-dialed participants. In this example, our dial plan is configured so that:

- all conference aliases for meetings start with **meet.**
- all users have a FindMe ID in the format **name.findme@domain.com**

We set up the TelePresence Conductor so that whenever anyone creates a conference based on a user's name (e.g. **meet.alice.findme@domain.com**), that user will automatically be dialed in to the conference via their FindMe ID (e.g. **alice.findme@domain.com**).

Step 1 - create a template

On the **Conference templates** page (**Conference configuration > Conference templates**, then click **New**):

Field	Input	Explanation
Name	meeting with FindMe	This template will be used whenever we want to automatically dial in a user's FindMe ID.
Description	template to route meetings to FindMe IDs	Descriptions are useful when you are managing a number of templates.
Conference type	*Meeting*	We want this template to apply to meetings only.

The rest of the settings on this page will depend on your network configuration.

Step 2 - create a conference alias

On the **Conference aliases** page (**Conference configuration > Conference aliases**, then click **New**):

Field	Input	Explanation	Example
Incoming alias (can use regular expression)	meet\.(.*\.findme@.*)	This regex will match any conference alias that begins with **meet.** and ends in **.findme@** followed by any domain name.	meet.alice.findme@domain.com
Conference name (can use regular expression)	\1	This replace string will result in **meet.** and **.findme@domain.com** being removed from the conference alias to create the conference name.	alice.findme@domain.com

The rest of the settings on this page will depend on your network configuration.

Step 3 - create an auto-dialed participant

On the **Auto-dialed participants** page (**Conference configuration > Auto-dialed participants**, then click **New**):

Field	Input	Explanation	Example
Name	FindMe user		
Description	dials user's FindMe ID in to meeting	Descriptions are useful if you are managing a number of auto-dialed participants.	

Field	Input	Explanation	Example
Conference template	*meeting with FindMe*	This is the name of the template that we created in Step 1.	
Conference name match	(.*\.findme@.*)	This regex will match against all possible conference names that include **.findme@** followed by any domain name.	alice.findme @domain.com
Address	\1	This replace string takes the conference name to create the address to be dialed.	alice.findme @domain.com

The rest of the settings on this page will depend on your network configuration.

Other examples that apply with this configuration:

- if a user dials **meet.bob.findme@domain.com** then **bob.findme@domain.com** will be dialed in to the resulting conference
- if a user dials **meet.carol.jones.findme@domain.com** then **carol.jones.findme@domain.com** will be dialed in to the resulting conference

Conference layouts

When creating a conference template or an auto-dialed participant, one of the parameters that can be set and passed to the conference bridge is the conference layout. Below are two tables displaying the layout families and specific layouts that can be selected.

Layout families

The <*index*> values for **`family<index>`** correspond to the following pane arrangements:

Layout families

index	Example layouts
1	
2	
3	
4	
5	

Specific layouts

The <*index*> values for **`layout<index>`** correspond to the following pane arrangements:

Specific layouts

index	Layout	index	Layout	index	Layout	index	Layout
1		16		31		46	
2		17		32		47	
3		18		33		48	
4		19		34		49	
5		20		35		50	
6		21		36		51	
7		22		37		52	
8		23		38		53	
9		24		39		54	
10		25		40		55	
11		26		41		56	
12		27		42		57	
13		28		43		58	
14		29		44		59	
15		30		45			

Port reference

The TelePresence Conductor uses different IP ports and protocols for different services and functions, and many of these are configurable. The table below lists each of these services and functions. For each, it shows the default port(s) and protocol used and whether these ports are used for inbound or outbound communications. If the ports are configurable it shows the available range and how to configure them using the web interface.

The information in the table below shows all possible services and the generic defaults for each. The actual services and ports used on your system will vary depending on its configuration, the option keys installed and features that have been enabled.

Note: two services or functions cannot share the same port and protocol; if you attempt to change an existing port or range and it conflicts with another service, an alarm will be raised.

Service/ function	Description	Default	Direction	Configurable via
SSH	Used for encrypted command line administration.	22 TCP	inbound	not configurable
NTP	Used for updating the system time (and important for H.235 security).	123 UDP	outbound	not configurable
SNMP	Used for network management.	161 UDP	inbound	not configurable
HTTP	Used for unencrypted web administration. Redirects HTTP requests to HTTPS.	80 TCP	inbound	not configurable
HTTPS	Used for encrypted web administration.	443 TCP	inbound and outbound	not configurable
Clustering	Used for communication between cluster peers	4369-4380 TCP	inbound and outbound	not configurable
Clustering	Used to recover from intra-cluster communication failure	4371 UDP	inbound	not configurable
Clustering	Used for IPsec secure communication between cluster peers.	500 UDP	inbound	not configurable
DNS	Used for sending requests to DNS servers.	uses a TCP source port from the ephemeral range		
HTTP	Used for outbound connection to the MCUs API.	uses a TCP source port from the ephemeral range		
HTTPS	Used for outbound connection to the MCUs API.	uses a TCP source port from the ephemeral range		
Remote logging	Used to send messages to the remote syslog server.	uses a TCP source port from the ephemeral range		
Login authentication	Used to connect to an LDAP server for login account authentication.	uses a TCP source port from the ephemeral range		

Event Log reference

This section provides the following reference information about the Event Log:

- Event Log format describes the structure of the Event Log.
- Message details list all the possible elements within the **message_details** field of the Event Log, in the order that they would normally appear, along with a description of each.

Event Log format

The Event Log is displayed in an extension of the UNIX syslog format:

```
date time process_name: message_details
```

where:

Field	Description
date	The local date on which the message was logged.
time	The local time at which the message was logged.
process_name	The name of the program generating the log message. This could include: ■ web for all web login and configuration events ■ conferencefactory.controller ■ conferencefactory.switchboard
message_details	The body of the message (see Message details for further information).

Message details

For most messages appearing in the event log, the **message_details** section, which contains the body of the message, consists of a number of human-readable **name=value** pairs, separated by a space.

The first elements within the **message_details** field are always **Level** (where applicable) and **Event**; the last name element is always **UTCTime**.

The table below shows all the possible name elements within the **message_details** field, in the order that they would normally appear, along with a description of each. The actual elements that appear will depend on the nature of the event.

Note: in addition to the events described below, a **syslog.info** event containing the string `MARK` is logged after each hour of inactivity to provide confirmation that logging is still active.

Name	Description
Level	The classification of the event. This could be one of: ■ **ERROR**: A condition has occurred that will affect the performance of the TelePresence Conductor but it will continue to function to some extent. ■ **WARNING**: A condition has occurred that may affect the performance of the TelePresence Conductor but it will continue to function to some extent. ■ **INFO**: Information messages. ■ **DEBUG**: Information that Cisco TAC engineers may use for debugging.
Event	The event which caused the log message to be generated.
Adhoc_chair_count	The number of conference bridge ports that are currently being used by participants (excluding any auto-dialed participants) who have a role of Chairperson.

Name	Description
Auto-dial_ participant_ address	The address of the auto-dialed participant.
Auto-dial_ participant_ keep_alive	The setting of the **Keep conference alive** field for this auto-dialed participant
Auto-dial_ participant_match	The string or regular expression used in the **Conference name match** field for the auto-dialed participant.
Auto-dial_ participant_ protocol	The protocol configured for this auto-dialed participant.
Auto-dial_ participant_role	The role assigned to this auto-dialed participant.
Auto-dial_ participant_rule	The string or regular expression used in the **Address** field for the auto-dialed participant.
Command	A command sent from TMS to the conference bridge via the TelePresence Conductor.
Conference_ alias_description	The description of the conference alias.
Conference_ alias_name	The name of the conference alias.
Conference_ alias_UUID	The unique identifier of the conference alias.
Conference_ name	The name of the conference.
Conference_ name_rule	The string or regular expression used in the **Conference name** field for the conference alias.
Conference_ part_type	Whether the conference is a primary conference, or a sub-conference (hosted on a cascade conference bridge).
Conference_ template_name	The name of the conference template.
Conference_ template_UUID	The unique identifier of the conference template.
Config_good	Indicates whether the basic configuration of the TelePresence Conductor is considered to be good.
Current_time	For application failure events, the current time (used to compare with the **Last_modified** time.
Detail	Descriptive detail of the Event.
Dst-alias	The alias received from the VCS.
Id	The UUID (unique identifier) of the alarm.
Incoming_alias_ match	The string or regular expression used in the **Incoming alias** field for the conference alias.
Last_modified	The time that the file was last modified.

Name	Description
MCU_address	The IP address or FQDN of the MCU.
MCU_ conference_ name	The name of the conference as it appears on the MCU. This will be the same as the conference name used by the TelePresence Conductor unless it is longer than 31 characters. See Conference name length for more information.
MCU_UUID	The unique identifier of the MCU.
Module	The module to which the event relates.
Participant_ address	The address of the participant used by the conference bridge.
Participant_name	The name of the participant used by the conference bridge.
Participant_ protocol	The protocol (H.323 or SIP) configured for this participant.
Participant_role	The role given to the participant by the TelePresence Conductor.
Participant_type	Whether the conference bridge considers the participant to be *scheduled* or *ad hoc*.
Phase	Whether the conference is in deleting or deleted state.
Reason	Textual string containing any reason information associated with the event.
Reserved_ adhoc_chair_ ports	The number of conference bridge ports that have been reserved for participants (excluding any auto-dialed participants) who have a role of Chairperson.
Severity	The level of severity of the alarm. See Alarm severity for definitions.
Source_address	The address of the endpoint used to place the call.
Source_protocol	The protocol (H.323 or SIP) used to place the call.
Source_ registered_alias	The registered alias of the endpoint used to place the call.
Status_good	Indicates whether the basic status of the TelePresence Conductor (including conference bridges and cluster peers) is considered to be good.
Tag	The call tag. This unique identifier is common to all forks of a call across a network of TelePresence Conductors and VCSs. See Call Tags for more information.
Unauthenticated_ source_alias	The unauthenticated alias of the endpoint used to place the call.
User	The username that was entered when a login attempt was made.
UTCTime	Time the event occurred, using a full UTC timestamp in YYYY-MM-DD HH:MM:SS,SSS format. Using this format permits simple ASCII text sorting/ordering to naturally sort by time. This is included due to the limitations of standard syslog timestamps.

Restoring default configuration

It is possible to restore the TelePresence Conductor to its default factory configuration, with the options of retaining the existing IP configuration and the root and administrator account passwords.

CAUTION: this procedure cannot be reversed and you will lose your current configuration. We recommend that you create a backup of the configuration before restoring the default configuration.

To restore the system to its default configuration:

1. Using SSH or a serial connection, log in to the TelePresence Conductor as **root**.
2. Type **factory-reset**
3. The following text appears:

```
**************************************************************************-
****
Warning! This operation resets the unit to factory default settings!
**************************************************************************-
****
To cancel operation before final confirmation press Ctrl+C
Keep option keys [YES/NO]?
```

4. Follow the prompts on the screen, typing **YES** or **NO** as appropriate to each option.

A description of each of the options is given in the table below.

Option	Description
Keep option keys	The TelePresence Conductor does not currently use option keys, so you can type either **YES** or **NO**.
Keep IP configuration	**YES** retains the system's IPv4 address, subnet mask and gateway.
Keep ssh keys	**YES** retains the system's SSH identity. Do this if you want to be sure that the system is identifying itself to other systems in the same way it did before the factory reset. **Note:** changes to a system's SSH identity may lead to other systems thinking that its identity is being spoofed.
Keep root and admin passwords	**YES** retains the existing passwords for the root and administrator accounts.
Save log files	**YES** saves the system's log files, including the latest rotation of the Event Log, to the hard disk where they can be retrieved by Cisco customer support if required.
Replace hard disk	**YES** pauses the factory reset process so that you can replace the system's hard disk. This option should be selected only on advice from Cisco customer support.
Are you sure you want to continue	**YES** starts the factory reset process with the selected options. To abort the factory reset process, type **NO**.

Identifying calls across your network

Call Tags

Call Tags are UUIDs that are used to track calls passing through a network of Cisco TelePresence Conductor and Cisco TelePresence Video Communication Servers (VCSs). When a VCS receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the VCS will use the existing Call Tag; if not,

it will assign a new Call Tag to the call. This Call Tag is then included in the call's details when the call is forwarded on to another VCS or a TelePresence Conductor. A single call passing between two or more VCSs and TelePresence Conductors can be identified as the same call by use of the Call Tag.

Note: Call Tags are supported by Cisco TelePresence Video Communication Server version X3.0 or later and all versions of Cisco TelePresence Conductor. If a call passes through a system that is not a VCS or TelePresence Conductor, or a VCS that is running an earlier version of the software, the Call Tag information will be lost.

Password encryption

All passwords configured on the TelePresence Conductor are stored in encrypted form. This applies to the following, which all have usernames and passwords associated with them:

- the default *admin* administrator account
- outbound connection credentials (used by the TelePresence Conductor when required to authenticate with another system)
- LDAP server (used by the TelePresence Conductor when binding to an LDAP server)

When entering or viewing passwords using the web interface, you will see placeholder characters (e.g. dots or stars, depending on your browser) instead of the characters you are typing.

Maximum length of passwords

When a password is encrypted, it uses more characters than the original plain text version of the password. For each type of password, the maximum number of plain text characters that can be entered and the maximum number of encrypted characters that are displayed through the CLI are shown in the table below.

Password type	Maximum plain text characters	Maximum displayed encrypted characters
Admin account	16	65
Outbound connection credentials	128	215
LDAP server	60	122

Flash status word reference table

The flash status word is used in diagnosing NTP server synchronization issues.

It is displayed by the `ntpq` program `rv` command. It comprises a number of bits, coded in hexadecimal as follows:

Code	Tag	Message	Description
0001	TEST1	pkt_dup	duplicate packet
0002	TEST2	pkt_bogus	bogus packet
0004	TEST3	pkt_unsync	server not synchronized
0008	TEST4	pkt_denied	access denied
0010	TEST5	pkt_auth	authentication failure
0020	TEST6	pkt_stratum	invalid leap or stratum
0040	TEST7	pkt_header	header distance exceeded
0080	TEST8	pkt_autokey	Autokey sequence error
0100	TEST9	pkt_crypto	Autokey protocol error
0200	TEST10	peer_stratum	invalid header or stratum
0400	TEST11	peer_dist	distance threshold exceeded
0800	TEST12	peer_loop	synchronization loop
1000	TEST13	peer_unreach	unreachable or nonselect

Alarm categories

The table below lists the possible alarm categories that can be raised on the TelePresence Conductor. Each alarm is identified by a 5-digit **Alarm ID**. The first 2 digits of the **Alarm ID** categorize the alarm as follows:

Alarm ID prefix	Category
10nnn	Hardware issues
15nnn	Software issues
20nnn	Cluster-related issues
25nnn	Network and network services settings
30nnn	Licensing / resources / option keys
35nnn	External applications and services (such as policy services or LDAP/AD configuration)
40nnn	Security issues (such as certificates, passwords or insecure configuration)
50nnn	General TelePresence Conductor configuration issues
55nnn	B2BUA issues

Bibliography

All documentation for the latest version of TelePresence Conductor can be found at www.cisco.com.

Title	Reference	Link
Cisco TelePresence Conductor Cluster Creation and Maintenance Deployment Guide	D14828	www.cisco.com
Cisco TelePresence Conductor Deployment Guide	D14827	www.cisco.com
Cisco TelePresence Conductor Getting Started Guide	D14829	www.cisco.com
Cisco TelePresence MCU Online Help	D14845	www.cisco.com
Cisco TelePresence MCU Series API Reference Guide	D14626	www.cisco.com
Cisco TelePresence Video Communication Server Administrator Guide	D14049	www.cisco.com
Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide	D14602	www.cisco.com
Cisco TelePresence Video Communication Server Multiway Cisco TelePresence Deployment Guide	D14366	www.cisco.com
Management Information Base for Network Management of TCP/IP-based internets: MIB-II		http://tools.ietf.org/html/rfc1213
Network Time Protocol website		www.ntp.org/
Regular Expression Pocket Reference, ISBN-10: 0596514271, ISBN-13: 978-0596514273		
RFC 1305: Network Time Protocol (Version 3) Specification, Implementation and Analysis		http://tools.ietf.org/html/rfc1305
RFC 2460: Internet Protocol, Version 6 (IPv6) Specification		http://tools.ietf.org/html/rfc2460
RFC 3164: The BSD syslog Protocol		http://tools.ietf.org/html/rfc3164
RFC 3880: Call Processing Language (CPL): A Language for User Control of Internet Telephony Services		http://tools.ietf.org/html/rfc3880
RFC 791: Internet Protocol		http://tools.ietf.org/html/rfc791
What warnings do I get on a Cisco TelePresence MCU that my conference is finishing? (knowledge base article)		www.cisco.com

Glossary

Term	Definition
Ad hoc participant	A participant who joins the conference by dialing a conference alias (see also Auto-dialed participant).
Alias	The name an endpoint uses when registering with the Cisco TelePresence Video Communication Server (VCS). Other endpoints can then use this name to call it. An endpoint may register with more than one alias.
Auto-dialed participant	A participant whose address is automatically dialed by the conference bridge when the conference starts (cf. Ad hoc participant). The address could relate to a device such as an endpoint or recording device, or could be a FindMe ID. For more information, see Creating and editing auto-dialed participants.
Call Policy	In relation to your video network, call policy is a set of rules that determine the action(s) to be applied to calls matching a given criteria. For more information, see Using Call Policy.
Call Tag	A UUID common to all forks of a call across a network of TelePresence Conductors and VCSs. See Call Tags for more information.
Cascade	The part of a conference that is being hosted on a secondary Cisco MCU. Conferences are cascaded to a secondary MCU when the primary MCU does not have enough ports available for all the participants. For more information, see Cascade ports.
Cluster	A collection of two or three TelePresence Conductor units that have been configured to work together in order to provide redundancy.
Chairperson	A participant who can control certain aspects of the conference and send content video such as a presentation. For more information, see About Chairperson and Guest roles.
Conference	In relation to this guide, a conference is a communication between multiple participants using voice, video or shared data presentation (or a combination of all three) from endpoints connected to a conference bridge using protocols such as H.323 and SIP, which are designed to negotiate audio-visual communication. The TelePresence Conductor allows users to create two types of conferences: *Meetings* and *Lectures*.
Conference alias	From the perspective of a conference participant, a conference alias is the string they need to dial to access a conference on the TelePresence Conductor. From the perspective of a TelePresence Conductor administrator, a conference alias is a set of rules that determines what happens when the TelePresence Conductor receives that particular alias (for example, the name of the conference and the role assigned to the participant). For more information, see Creating and editing conference aliases.
Conference bridge	A network device that allows multiple endpoints to participate in a video conference, for example an MCU (Multipoint Control Unit).

Term	Definition
Conference bridge pool	A conference bridge pool is a collection of conference bridges, all of the same type and with the same configuration. The TelePresence Conductor treats a pool of conference bridges as a single conference bridge resource, increasing the available capacity and providing redundancy. Grouping conference bridges into pools according to categories (such as geographical location, installed language localization kit or port type, e.g. HD/SD) also allows you to specify that different sets of conference bridges are used in different situations. For more information, see Managing conference bridges and Selecting the preferred conference bridges for a conference.
Conference bridge type	The type of multipoint-conference bridge. This release of the TelePresence Conductor supports *Cisco TelePresence MCUs* only. Future versions may support other types of conference bridges.
Conference type	There are two types of conferences: *Meetings* and *Lectures*. **Meetings** have one type of participant (*Participant*). All participants have the same Chairperson-level privileges and default settings, determined by the configuration for the Chairperson role on the conference bridge. **Lectures** have two types of participants (*Chairperson* and *Guest*). Each has potentially different privileges and default settings, determined by the configuration of these respective roles on the conference bridge.
Dial plan	A dial plan defines all the possible aliases and call routes within your video network. For more information, see Designing a dial plan.
External manager	The remote system that is used to manage endpoints and network infrastructure. The Cisco TelePresence Management Suite (TMS) is an example of an external manager.
FQDN Fully Qualified Domain Name	A domain name that specifies the node's position in the DNS tree absolutely, uniquely identifying the system or device. Note that in order to use FQDNs instead of IP addresses when configuring the TelePresence Conductor, you must have at least one DNS server configured.
Guest	A participant who does not have Chairperson privileges on the conference bridge. For more information, see About Chairperson and Guest roles.
H.323	ITU signaling standard designed to establish connections for voice and video communications over an IP network.
Lecture	On the TelePresence Conductor, a lecture is a conference where there are two types of participant role (*Chairperson* or *Guest*). Each has potentially different privileges and default settings, determined by the configuration of these respective roles on the conference bridge.
Meeting	On the TelePresence Conductor, a meeting is a conference where there is just one type of participant role (namely *Participant*). All participants have the same privileges and default settings, determined by the configuration for the Chairperson role on the conference bridge.
Participant	A person or device who has joined a conference. Each participant: ■ will be either an ad hoc participant or an auto-dialed participant ■ will have a role of chairperson or guest (for lectures), or participant (which equates to chairperson) for meetings, and ■ may or may not be using a reserved port.

Term	Definition
Peer	A TelePresence Conductor unit that has been configured to belong to a cluster.
PEM Privacy-Enhanced Electronic Mail	An IETF proposal for securing messages using public key cryptography.
Primary conference bridge	The conference bridge on which a conference is initially created.
Regex Regular expression	A pattern used to match text strings according to a POSIX-defined syntax.
Reserved participant	A participant for whom a port has been specifically reserved. For this release of the TelePresence Conductor, it is possible to reserve ports for Chairpersons only. For more information, see Chairperson ports.
Secondary conference bridge	The conference bridge onto which a conference has been cascaded from a primary conference bridge.
Service Preference	A Service Preference is a prioritized list of conference bridge pools. If no conference bridges within the first pool can be used to host a conference (for example, if there are insufficient resources available for the requirements of the conference), the TelePresence Conductor will check whether the second pool in the list can be used, and so on. For more information, see Selecting the preferred conference bridges for a conference.
SIP Session Initiation Protocol	IETF protocol for controlling multimedia communication. Defined by *RFC 3261* [20].
Source alias	The alias present in the “source” field of a message.
TCS Cisco TelePresence Content Server.	A Cisco product which records Cisco TelePresence or third-party videoconferencing meetings and multimedia presentations for live broadcast and on-demand access.
TMS Cisco TelePresence Management Suite	A Cisco product used for the management of video networks.
VCS Video Communications Server	A generic term for the Cisco TelePresence Video Communication Server product which acts as a gatekeeper and SIP proxy/server.
VCS Control	A Cisco TelePresence Video Communication Server whose main function is to act as a gatekeeper, SIP proxy and firewall traversal client. This system is generally located within the firewall.
VCS Expressway	A Cisco TelePresence Video Communication Server with the same functionality as a VCS Control that can also act as a firewall traversal server. This is generally located outside the firewall.

Legal notices

Intellectual property rights

This Administrator Guide and the product to which it relates contain information that is proprietary to TANDBERG and its licensors. Information regarding the product is found below in the Copyright notice and Legal notices sections.

TANDBERG® is a registered trademark belonging to Tandberg ASA. Other trademarks used in this document are the property of their respective holders. This Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of this product. Except for the limited exception set forth in the previous sentence, no part of this Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG.

COPYRIGHT © TANDBERG

Copyright notice

The product that is covered by this Administrator Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

This product is Copyright © 2012, Tandberg Telecom UK Limited. All rights reserved.

TANDBERG is now part of Cisco. Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

A list of the conditions of use can be found at:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/conductor/license_info/Cisco_Conductor_EULA.pdf

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at:

http://www.cisco.com/en/US/products/ps11775/products_licensing_information_listing.html

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes software developed by the University of California, Berkeley and its contributors.

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

Accessibility notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco TelePresence Conductor is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence