Cisco TelePresence Conductor

Administrator Guide

XC2.1

D14826.05

May 2013

Contents

Introduction to the Cisco TelePresence Conductor 7

About the Cisco TelePresence Conductor 8

Cisco TelePresence Conductor features 8

What's new in this version? 8

Using the web interface 10

Logging in to the web interface 10

Web page features and layout 10

Supported browsers and characters 12

Using the TelePresence Conductor without a release key 13

Before you start 14

Configuring conference bridges for use with the TelePresence Conductor 15

Configuring call control device(s) for use with the TelePresence Conductor 16

Configuring endpoints for use with the TelePresence Conductor 17

Designing a dial plan 18

About dial plans 18

General considerations 18

Considerations in a Cisco VCS-only deployment 18

Configuration overview 20

Configuring TelePresence Conductor in a Cisco VCS deployment 20

Configuring TelePresence Conductor in a Unified CM deployment 22

Configuring system settings 27

System administration 28

HTTP Strict Transport Security (HSTS) 29

Configuration using the front panel 29

Ethernet 31

Status 31

IP configuration 32

Network configuration 32

Primary LAN 1 IP address 32

Additional IP addresses for LAN1 32

DNS 33

DNS settings 33

DNS servers 34

Time 35

Configuring the NTP servers 35

Displaying NTP status information 35

TelePresence Conductor time display and time zone 36

SNMP 38

Configuring firewall rules 40

Setting up and activating firewall rules 41

Current active firewall rules 43

Managing conference bridges 44

About conference bridges 45

Creating conference bridge pools 46

Adding and editing conference bridges 48

Busying out conference bridges 50

Deleting conference bridges 51

Viewing all conference bridges across all pools ... 52
Moving a conference bridge between pools ... 53
Adding or editing quality settings ... 54
Changing global conference bridge settings ... 55
Changing the conference bridge retry interval ... 55
Setting the threshold for raising conference bridge resource usage alarms ... 55
Conference bridge response time ... 57

Configuring conferences ... 58

Using the basic conference configuration wizard ... 59
Selecting the preferred conference bridges for a conference ... 60
Creating a Service Preference ... 60
Cascading conferences across conference bridges and conference bridge pools ... 62
Creating and editing conference templates ... 63
Adding and editing advanced template parameters ... 67
About resource allocation ... 73
Resource reservation and allocation on the TelePresence MCU ... 73
Resource reservation and allocation on the TelePresence Server ... 74
Limiting the number of participants in a conference ... 77
Creating and editing conference aliases ... 78
Conference name length ... 79
Creating and editing auto-dialed participants ... 80
Using auto-dialed participants and Multiway ... 82
Sending DTMF tones to an auto-dialed participant ... 82
What if an auto-dialed participant cannot be reached? ... 82
Adding and editing advanced auto-dialed participant parameters ... 83
About chairperson and guest roles ... 87
Assigning roles ... 87
Differences between chairperson and guest roles ... 87
Creating and editing Unified CM locations ... 89
Adding auto-dialed participants to Unified CM for Ad hoc conferences ... 90
Creating and editing pre-configured endpoints ... 91
Adding and editing pre-configured endpoint codecs ... 93
Using Call Policy ... 95
About Call Policy ... 95
When to use Cisco VCS or TelePresence Conductor Call Policy ... 95
Defaults ... 95
Configuring Call Policy ... 95
Example usage ... 96

Configuring users ... 98

Configuring administrator accounts ... 99
Configuring remote account authentication using LDAP ... 101
Connection status ... 102
Configuring administrator groups ... 104
Password security ... 106
Configuring the root account ... 107
Changing the root account password ... 107
Enabling and disabling access over SSH ... 107
Resetting forgotten passwords ... 108
Resetting your administrator password if you still have access to the root account ... 108
Resetting an administrator password or your root password via a serial connection ... 108

Viewing status **109**
Getting a status overview 110
Alarms 111
Viewing alarms 111
Actioning alarms 111
Acknowledging alarms 111
Deleting alarms 111
Alarm information 111
Alarm severity 112
Conference bridge status 113
Conferences status 114
Conference participants 115
Call status information 116
Call status 116
Event Log 117
About the Event Log 117
Filtering the Event Log 117
Reconfiguring the log settings 117
Viewing events 118
Event Log color coding 118
Configuration Log 119
Filtering the Configuration Log 119
Results section 119

Clustering **120**
About clusters 121
Peer IP addresses 121
Cluster pre-shared key 121
Peer-specific configuration 122
Cluster configuration 122
Ethernet 122
IP 122
System host name and domain 122
DNS servers 122
Time 122
SNMP 123
Logging 123
Security certificates 123
Administration access 123
Root account password 123
Unified CM locations 123
Creating a new cluster 124
Prerequisites 124
Placing the initial peer into cluster mode 124
Adding new peers to the cluster 125
Updating configuration on the call control devices 125
Monitoring the status of the cluster 126
Changing a peer's IP address 127
Removing a peer from an existing cluster 128
Removing a live peer from a cluster 128
Removing an out-of-service peer from a cluster 128

Placing the peer in standalone mode ... 128
Removing the peer from the cluster ... 129
Disbanding a cluster ... 130
Upgrading a cluster ... 131
Cluster backup and restore ... 132
Maintenance ... 133
About upgrading software components ... 134
Before you upgrade ... 134
Upgrading using the web interface ... 135
Upgrading using secure copy (SCP/PSCP) ... 136
Logging configuration ... 137
About the Event Log ... 137
Remote logging of events ... 137
Add option and release keys ... 138
About the Tools menu ... 139
Check pattern ... 139
Check dial plan ... 140
Ping ... 140
Traceroute ... 141
Tracepath ... 141
DNS lookup ... 142
Trusted CA Certificate ... 144
Managing the TelePresence Conductor's server certificate ... 145
Server certificates and clustered systems ... 146
Backing up and restoring data ... 147
Backing up and restoring overview ... 147
Creating a backup ... 148
Restoring a previous backup ... 148
Diagnostic logging ... 149
Clustered systems ... 149
Creating a system snapshot ... 151
Incident reporting ... 152
Incident reporting caution: privacy-protected personal data ... 152
Sending incident reports automatically ... 152
Sending incident reports manually ... 153
Viewing incident reports ... 153
Incident report details ... 154
Viewing or deleting feedback receivers ... 155
Restarting, rebooting and shutting down ... 156
Developer resources ... 158
Debugging and system administration tools ... 158
Experimental menu ... 158
Reference ... 159
Software version history ... 160
XC2.0 ... 160
Regular expression reference ... 162
About regular expressions ... 162
Regular expression examples - conference aliases ... 163
Regular expression examples - Lectures ... 166
Regular expression examples - auto-dialed participants ... 166

Conference layouts 170
TelePresence MCU layouts 170
TelePresence Server layouts 171
Port reference 173
Event Log reference 174
Event Log format 174
Message details 174
Restoring default configuration 176
Identifying calls across your network 177
Call Tags 177
Password encryption 178
Maximum length of passwords 178
Flash status word reference table 179
Alarm categories 180
Bibliography 181
Glossary 182
Legal notices 186
Intellectual property rights 186
Copyright notice 186
Accessibility notice 187

Introduction to the Cisco TelePresence Conductor

This section introduces the Cisco TelePresence Conductor and its features.

About the Cisco TelePresence Conductor 8
Using the web interface 10
Using the TelePresence Conductor without a release key 13

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 conference bridge(s) and one or more call control device(s) (either Cisco TelePresence Video Communication Servers (VCSs) or Cisco Unified Communications Managers (Unified CMs)). It allows the video network to be configured such that spontaneous or rendezvous* conferences may be easily provisioned, initiated, accessed and managed.

* personal conferences with a unique conference ID that are 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. It will control all of these individual elements to achieve the best possible performance. This will ensure intelligent conference placement and improved resource utilization and provides powerful, comprehensive administrator control.

It is tightly integrated with the industry-leading Cisco TelePresence MCUs, the Cisco TelePresence Servers, the Cisco TelePresence Video Communication Servers (VCSs), the Cisco Unified Communications Managers (Unified CMs) and the Cisco TelePresence Management Suite (Cisco TMS). It will work with all standards-compliant endpoints.

The 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.

The TelePresence Conductor 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.

What’s new in this version?

The new features introduced in this release of the TelePresence Conductor software are described below:

Limited system capacity when running without a release key

The TelePresence Conductor can be run without a release key. In this mode the system capacity is limited; only a single un-clustered conference bridge can be enabled and the TelePresence Conductor cannot be clustered.

Where the TelePresence Conductor has no release key, only "community support" is available. This is a self / collaborative support effort, using technical forums like https://supportforums.cisco.com/community/netpro/collaboration-voice-video/telepresence. TAC support is

only available for TelePresence Conductors that have a release key; for further details see https://www.cisco.com/web/services/portfolio/product-technical-support/index.html.

For deployments in production environments we recommend that customers upgrade to a fully licensed installation of TelePresence Conductor.

Using the web interface

This section provides information on how to use the TelePresence Conductor web interface. It also describes what the web interface layout looks like and which browsers and characters are supported.

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 (fully-qualified domain name) of the system.

   The **Administrator login** page appears.
2. Enter a valid administrator **Username** and **Password** (see the Configuring administrator accounts [p.99] section for details on setting up administrator accounts) and click **Login**.

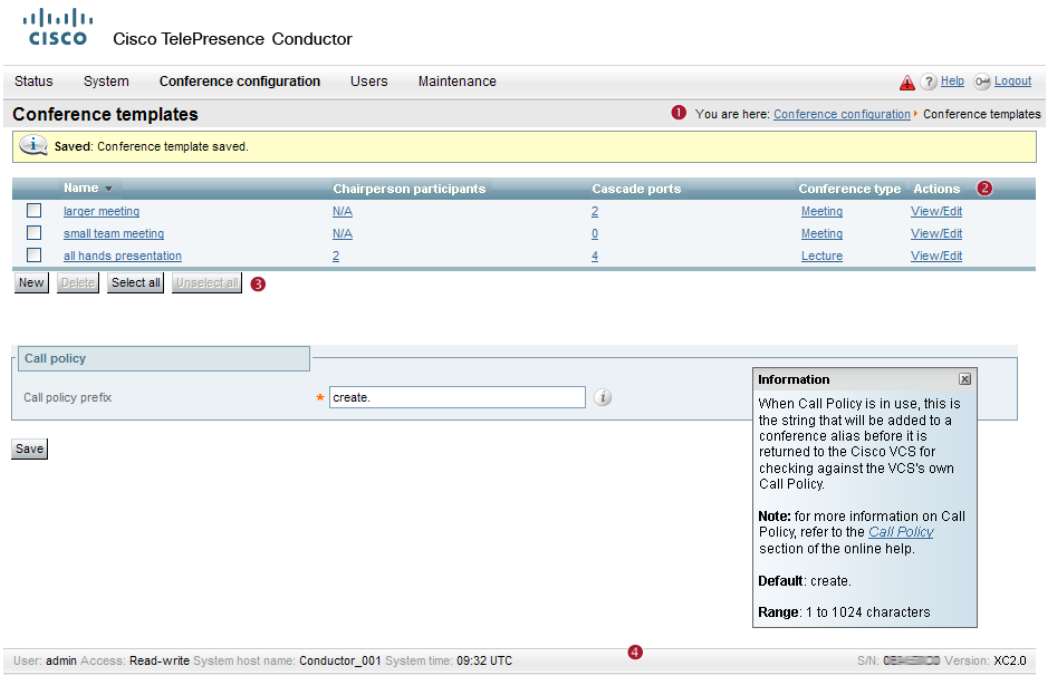
You are presented with the **Overview** page.

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.

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. See Managing the TelePresence Conductor's server certificate [p.145] for more information.

Web page features and layout

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



Example web page

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

Page element		Description
Page name and location	1	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 related to 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.
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 or descending order.

Page element		Description
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.

Supported browsers and characters

Supported browsers

The TelePresence Conductor web interface is designed for use with Internet Explorer 8 or 9, Firefox 3 or later, 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 (&)
- pipe symbol (|)

Case sensitivity

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

Using the TelePresence Conductor without a release key

It is possible to use the TelePresence Conductor without a valid release key. However, this results in limited system capacity. The limitations are:

- The TelePresence Conductor cannot be part of a cluster.
- Only one un-clustered conference bridge across all conference bridge pools can be enabled at a time. **Note:** conference bridges that are clustered are not supported. If a clustered conference bridge is enabled on the TelePresence Conductor it will be displayed as *Unusable* on the **Conference bridge status** page and the TelePresence Conductor cannot communicate with it.

When the TelePresence Conductor is running without a valid release key a banner is displayed along the top of the web interface, stating "**No Release key installed:** The TelePresence Conductor is running without a valid release key; system capacity will be limited. Contact your Cisco account representative to obtain release key and option keys."

Where the TelePresence Conductor has no release key, only "community support" is available. This is a self / collaborative support effort, using technical forums like https://supportforums.cisco.com/community/netpro/collaboration-voice-video/telepresence. TAC support is only available for TelePresence Conductors that have a release key; for further details see https://www.cisco.com/web/services/portfolio/product-technical-support/index.html.

For deployments in production environments we recommend that customers upgrade to a fully licensed installation of TelePresence Conductor. To buy a release key and take advantage of the full feature set, contact your Cisco support representative with the serial number of the TelePresence Conductor (displayed under **Maintenance > Option keys**).

Before you start

This section provides information on the other devices that need to be configured to work with the TelePresence Conductor, how to design a dial plan and a configuration overview.

Configuring conference bridges for use with the TelePresence Conductor 15
Configuring call control device(s) for use with the TelePresence Conductor 16
Configuring endpoints for use with the TelePresence Conductor 17
Designing a dial plan 18
Configuration overview 20

Configuring conference bridges for use with the TelePresence Conductor

A conference bridge is used for hosting the participants of a multipoint conference.

This version of the TelePresence Conductor supports the conference bridges Cisco TelePresence MCU (version 4.2 or later) and Cisco TelePresence Server (version 3.0 or later).

All conference bridges managed by a TelePresence Conductor must be added to a conference bridge pool that contains conference bridges of one 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. When the TelePresence Conductor receives a request for conference resources, it determines the conference bridge(s) that the conference should be hosted on.

All TelePresence Servers managed by the TelePresence Conductor must be configured to run in 'Remotely managed' mode.

All conference bridges in a single conference bridge pool must be configured identically before they are added to the TelePresence Conductor. The required configuration depends on whether the TelePresence Conductor is deployed in a setup using a Cisco VCS, a Unified CM or both.

For information on configuring a conference bridge in a Cisco VCS deployment, see *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server Deployment Guide* or *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server (B2BUA) Deployment Guide*.

For information on configuring a conference bridge in a Unified CM deployment see *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.

Configuring call control device(s) for use with the TelePresence Conductor

A call control device is used for managing the communication between SIP and/or H.323 devices.

This version of the TelePresence Conductor supports the call control devices Cisco TelePresence Video Communication Server (VCS) version X7.0 or later, and Cisco Unified Communications Manager (Unified CM) version 8.6.2 or later.

The Cisco VCS is supported in the following two types of deployments:

- Using the Cisco VCS's external policy service interface
  This method may be discontinued in future versions of the TelePresence Conductor software.
  For more information see *Cisco TelePresence Conductor with Cisco TelePresence VCS Deployment Guide*.
- Using the TelePresence Conductor's back-to-back user agent (B2BUA)
  This method requires a SIP trunk between the Cisco VCS and the TelePresence Conductor. It is the preferred method to use.
  For more information see *Cisco TelePresence Conductor with Cisco TelePresence VCS (B2BUA) Deployment Guide*.

For information on configuring a Unified CM for use with the TelePresence Conductor see *Cisco TelePresence Conductor with Cisco Unified Communications Manager 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 Cisco TelePresence Video Communication Server (Cisco VCS) or Cisco Unified Communications Manager (Unified CM), 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.

Designing a dial plan

About dial plans

A dial plan defines dialed aliases and call routes within your video network. A well-designed dial plan is a key component of a successful audio/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 on your Cisco VCS or Unified CM to ensure it supports the following aspects:

Area	Description
Conference aliases	These are the aliases that users will dial to create or join a conference. The conference aliases, which may be prefixes or exact matches, must be routed to the TelePresence Conductor. You will need to ensure that your dial plan routes these prefixes appropriately. For more information, see Creating and editing conference aliases [p.78].
Conference names	These are the names that each conference will be known by on the host conference bridge. For more information, see Conference name [p.78].
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 forward particular aliases to your recording device. For more information, see Creating and editing auto-dialed participants [p.80].

Considerations in a Cisco VCS-only deployment

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 Cisco VCS for checking against its own Call Policy. For more information, see Using Call Policy [p.95].
Conference bridge dial plan prefixes	These are used by the Cisco VCS to route calls to conference bridges in the TelePresence Conductor's pool. Each conference bridge must have a unique prefix. Each prefix must be configured on the VCS. For more information, see Dial plan prefix [p.50].

Area	Description
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 [p.165] 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 Cisco 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.
Avoiding a dial plan conflict	The Cisco VCS is responsible for routing calls to the appropriate destination (for example, TelePresence Conductor, TelePresence MCU, another Cisco VCS, or endpoint). It does this by employing search rules, which map search requests to zones and policy servers based on factors such as the alias being dialed and the source of the request. When creating your search rules on the Cisco 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 full instructions on creating transforms and configuring search rules on the Cisco VCS, see *Cisco TelePresence Video Communication Server Administrator Guide*.

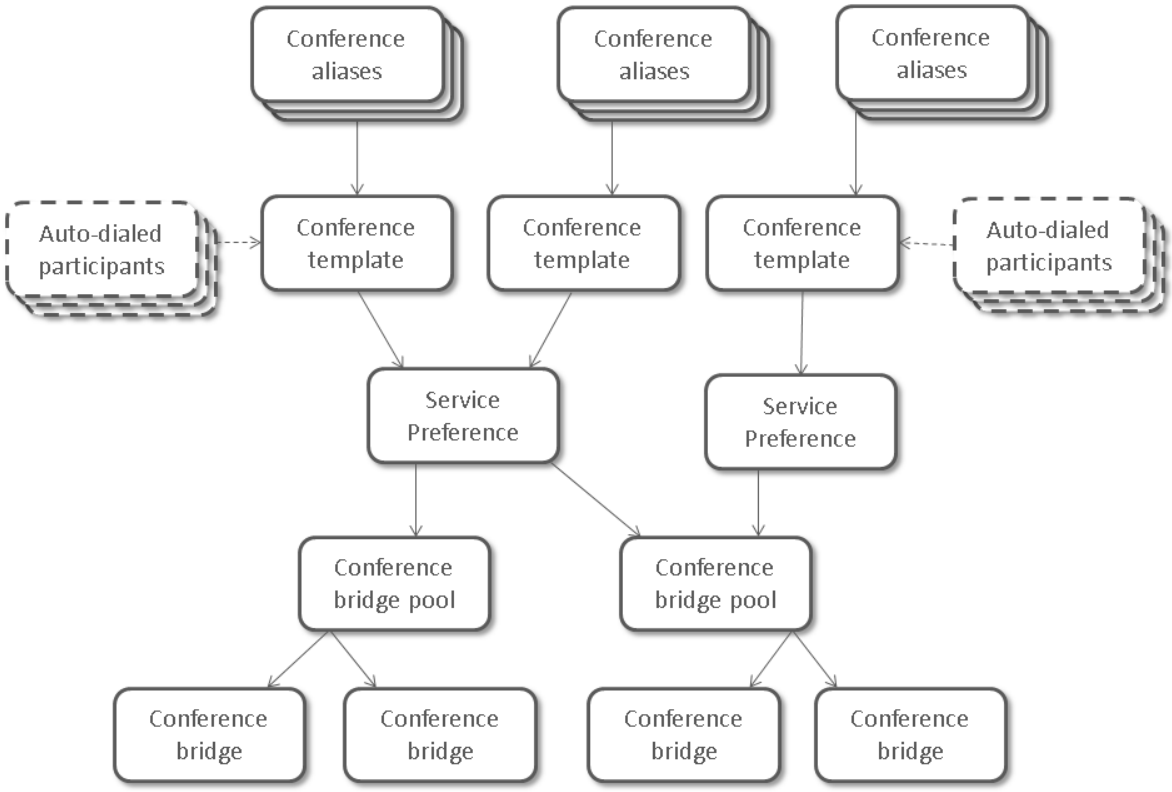
Configuration overview

TelePresence Conductor can be deployed with multiple Cisco VCSs or Unified CMs or a combination of the two. The configuration required on the TelePresence Conductor depends on the deployment.

Configuring TelePresence Conductor in a Cisco VCS deployment

In a Cisco VCS deployment a Rendezvous 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.

Configuring Rendezvous conferences that use the Cisco VCS's external policy service interface

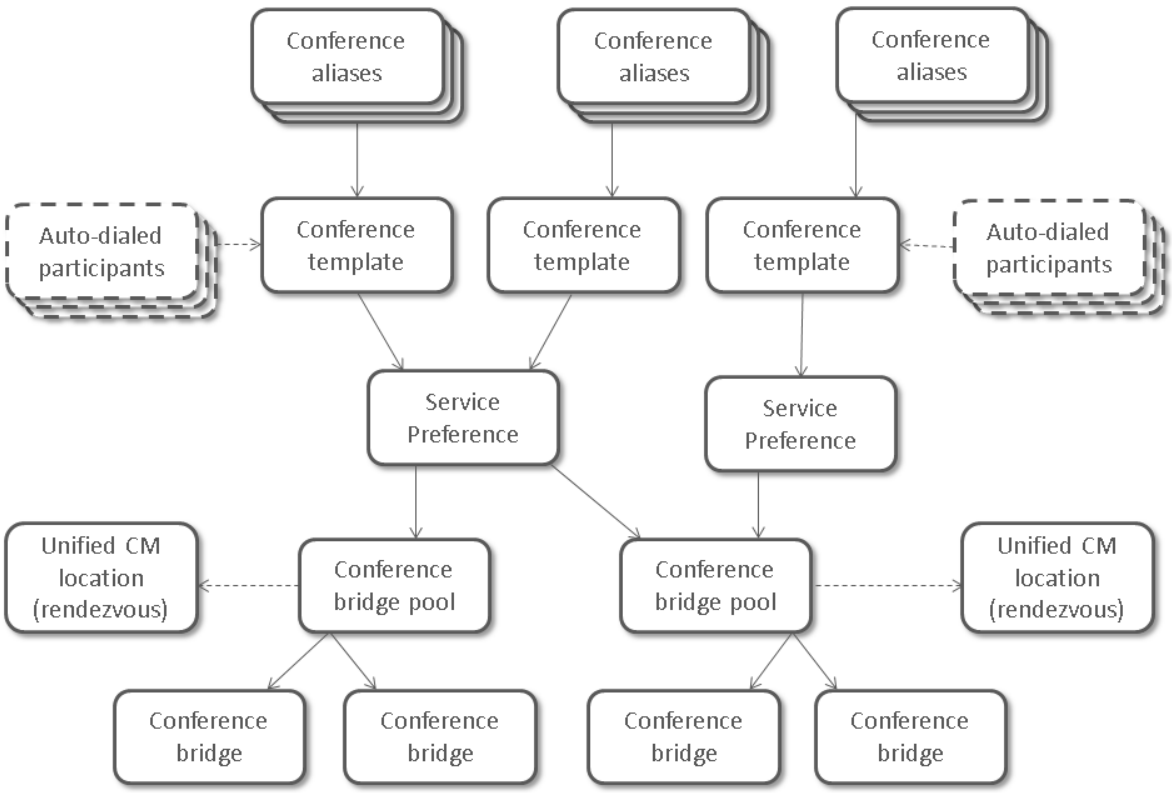


To configure a Rendezvous conference in a Cisco VCS deployment using the Cisco VCS's external policy server interface:

1. Ensure that all the Cisco 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 the *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server Deployment Guide*.

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 when a large number of resources is needed.
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, recording devices or even voice bridges.

Configuring Rendezvous conferences that use the TelePresence Conductor's B2BUA



To configure a Rendezvous conference in a Cisco VCS deployment using the TelePresence Conductor's back-to-back user agent (B2BUA):

1. Ensure that all the Cisco 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 the *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server (B2BUA)*

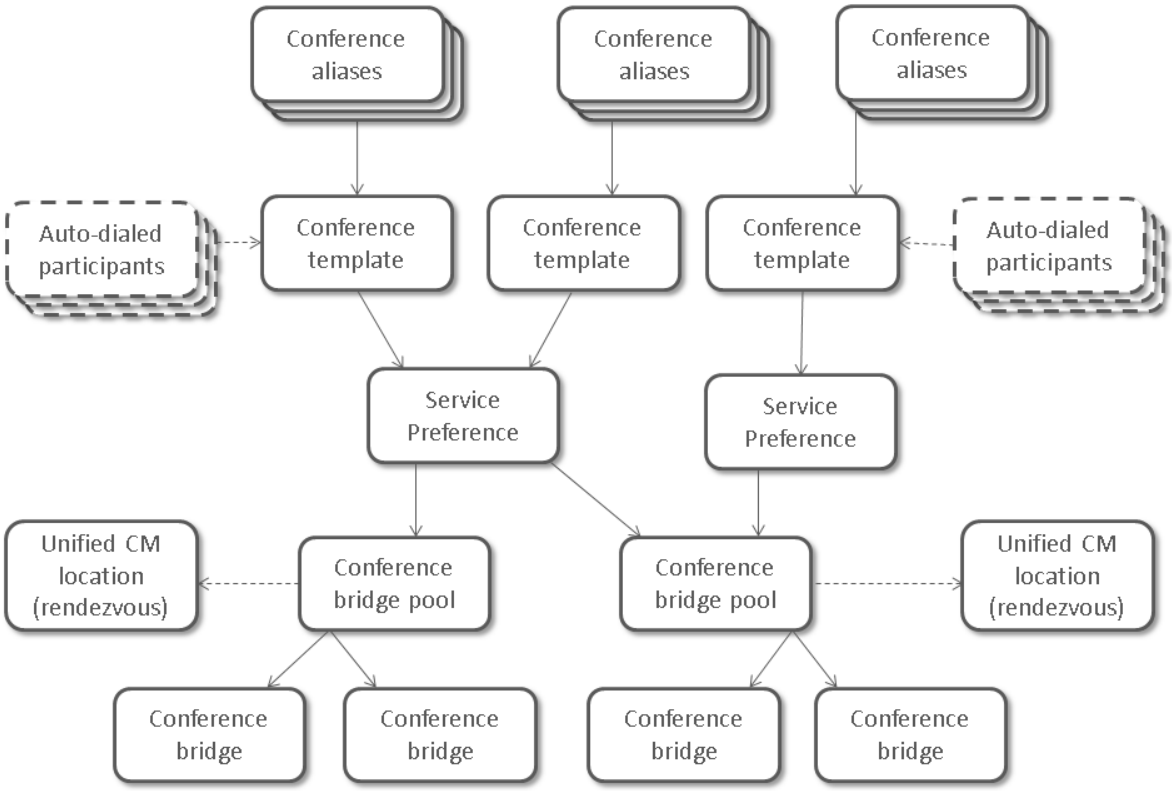
Deployment Guide.

2. Add one local Rendezvous IP address that the Cisco VCS connects to in order to create Rendezvous conferences on the TelePresence Conductor.
3. Add one Unified CM location for all Cisco VCSs that the TelePresence Conductor connects to via a SIP trunk. Each Unified CM location references a local Rendezvous IP address and a trunk IP address, protocol and port on the Cisco VCS that is used for outbound Rendezvous calls from the conference bridges.
4. Create one or more pools of conference bridges that the TelePresence Conductor will use for its conferences. Each pool, which contains conference bridges that make outbound calls to participants registered on a Cisco VCS, needs to reference a Unified CM location.
5. Add conference bridges to the pool. Each pool must contain at least one conference bridge. The conference bridge needs to have the correct SIP port for TLS defined. The default SIP port is 5061.
6. Set up at least one Service Preference, defining the order in which conference bridge pools will be used when a large number of resources is needed.
7. 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).
8. 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.
9. 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, recording devices or even voice bridges.

Configuring TelePresence Conductor in a Unified CM deployment

In a Unified CM deployment both Rendezvous and Ad hoc conferences can be configured. A Rendezvous conference is initiated when someone dials a pre-determined conference alias. An Ad hoc conference is initiated when two participants in a call add additional participants into a spontaneous conference.

Configuring Rendezvous conferences

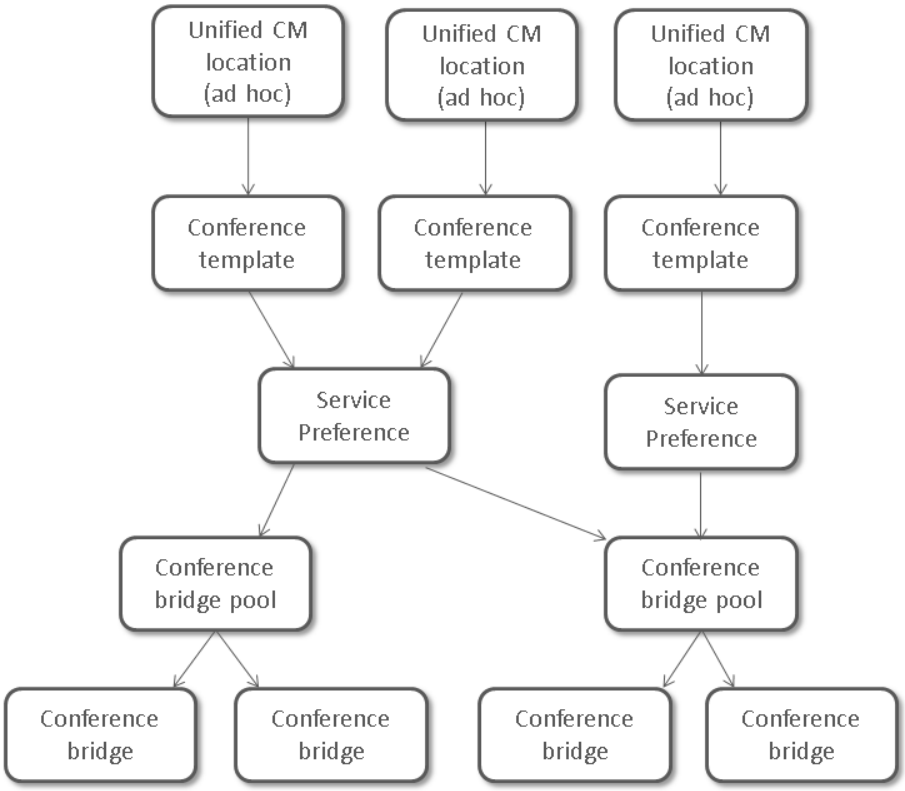


To configure a Rendezvous conference in a Unified CM deployment:

1. Ensure that all the Unified CMs 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 the *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.
2. Add all local Rendezvous IP addresses that the Unified CM connects to in order to create Rendezvous conferences on the TelePresence Conductor.
3. Add Unified CM locations for all locations in which Rendezvous conferences will be created. Each Unified CM location references a local Rendezvous IP address and a trunk IP address, protocol and port on the Unified CM that is used for outbound Rendezvous calls from the conference bridges.
4. Create one or more pools of conference bridges that the TelePresence Conductor will use for its conferences. Each pool, which contains conference bridges that make outbound calls to participants registered on Unified CM, needs to reference a Unified CM location.
5. Add conference bridges to the pool. Each pool must contain at least one conference bridge. The conference bridge needs to have the correct SIP port for TLS defined. The default SIP port is 5061.
6. Set up at least one Service Preference, defining the order in which conference bridge pools will be used when a large number of resources is needed.
7. 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).

8. 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.
9. 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, recording devices or even voice bridges.

Configuring Ad hoc conferences without auto-dialed participants

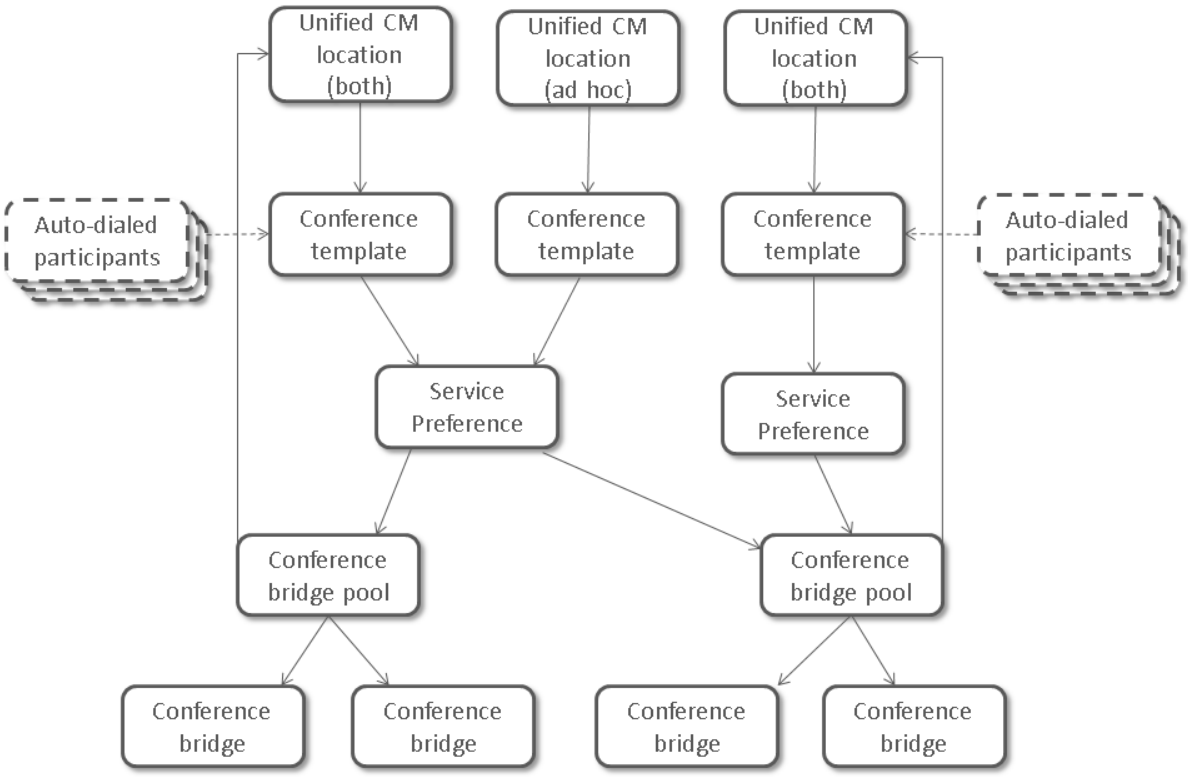


To configure an Ad hoc conference without any auto-dialed participants in a Unified CM deployment:

1. Ensure that all the Unified CMs 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 the *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.
2. Add all local Ad hoc IP addresses that the Unified CM connects to in order to create Ad hoc conferences on the TelePresence Conductor.
3. Create one or more pools of conference bridges that the TelePresence Conductor will use for its conferences.
4. Add conference bridges to the pool. Each pool must contain at least one conference bridge. The conference bridge needs to have the correct SIP port for TLS defined. The default SIP port is 5061.
5. Set up at least one Service Preference, defining the order in which conference bridge pools will be used when a large number of resources is needed.

6. 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).
7. Add or update Unified CM locations for all locations in which Ad hoc conferences will be created. Each Unified CM location references a local Ad hoc IP address and a conference template.

Configuring Ad hoc conferences with auto-dialed participants



To configure an Ad hoc conference with auto-dialed participants in a Unified CM deployment:

1. Ensure that all the Unified CMs 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 the *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.
2. Add all local Ad hoc and Rendezvous IP addresses that the Unified CM connects to in order to create Ad hoc conferences on the TelePresence Conductor. The Rendezvous IP addresses are used as the TelePresence Conductor's source IP address for outbound calls.
3. Create one or more pools of conference bridges that the TelePresence Conductor will use for its conferences.
4. Add conference bridges to the pool. Each pool must contain at least one conference bridge. The conference bridge needs to have the correct SIP port for TLS defined. The default SIP port is 5061.
5. Set up at least one Service Preference, defining the order in which conference bridge pools will be used when a large number of resources is needed.

6. 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).
7. Add or update Unified CM locations for all locations in which Ad hoc conferences will be created. Select a conference type of *Both*, to allow for configuration of the inbound Ad hoc and outbound SIP trunk. Each Unified CM location needs to reference a local Ad hoc IP address, a conference template, a local Rendezvous IP address (the source IP address of the SIP trunk to Unified CM), and trunk settings for the Unified CM (for outbound calls).
8. Go back to the conference bridge pool that is used for this Ad hoc conference and link it to the Unified CM location created above.
9. Define any auto-dialed participants for this Ad hoc conference.

Configuring system settings

This section provides information on how to configure the system settings on the TelePresence Conductor, accessible via the **System** menu.

System administration 28
Ethernet 31
IP configuration 32
DNS 33
Time 35
SNMP 38
Configuring firewall rules 40
Current active firewall rules 43

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
Session time out (minutes)	Sets the number of minutes that an administration session (via serial port, HTTPS or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off. **Default:** 30
Per-account session limit	The number of concurrent sessions that each individual administrator account is allowed on the system. This includes web, SSH and serial port sessions. A value of 0 turns session limits off. **Default:** 0
System session limit	The maximum number of concurrent administrator sessions allowed on the system. This includes web, SSH and serial port sessions. A value of 0 turns session limits off. **Default:** 0
Serial port / console	Determines whether the system can be accessed locally via either the serial DATA port (for a physical system) or VMware console (for a virtual machine). The `pwrec` command to reset the root or administrator password is still available for one minute after a reboot, even if the Serial port has been turned off. Note that there is no tsh support on TelePresence Conductor. **Default:** On
SSH service	Determines whether the TelePresence Conductor can be accessed via SSH and SCP. **Default:** On
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 the product name (Cisco TelePresence Conductor), the LAN 1 IPv4 address, and any alarms that may apply to the unit. It is also possible to configure the IP settings and reboot the TelePresence Conductor unit via the LCD panel. For details on this see Configuration using the front panel [p.29]. *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 October 2012, this mechanism is supported by the following browsers:

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

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

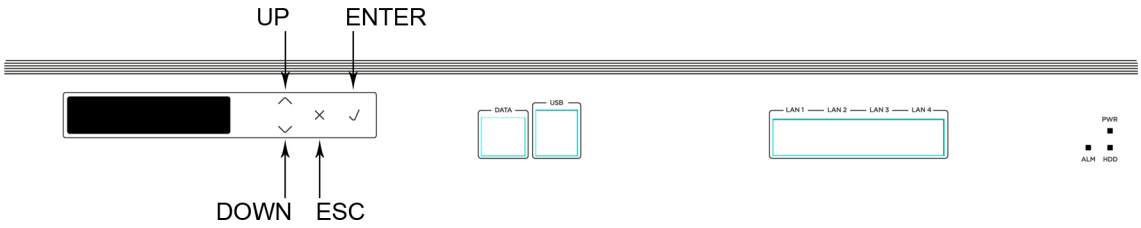
- Automatically turn any insecure links to the website into secure links (for example, **`http://example.com/page/`** is modified to **`https://example.com/page/`** before accessing the server).
- Only allow access to the server if the connection is secure (for example, the server's TLS certificate is 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).

Configuration using the front panel

The LCD panel and buttons at the front of the TelePresence Conductor allow you to configure and check the IP settings as well as to reboot the system. We do not recommend that you perform the initial configuration using the front panel, but you may need to use this method if you do not have access to a PC and serial cable.



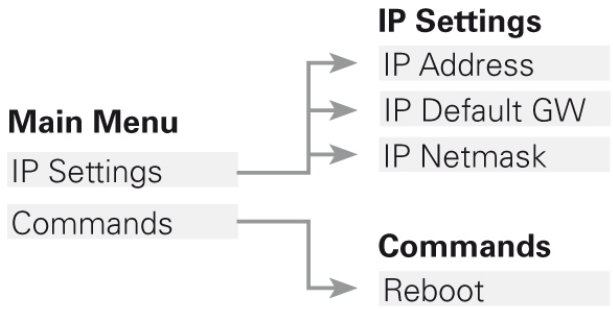
By default, during normal operation the front panel of the TelePresence Conductor unit shows a rotating display of the Cisco TelePresence Conductor's system name, the LAN 1 IPv4 address, and any alarms that may apply to the unit.

To control the display of status items:

- **`ENTER`** stops the display from automatically rotating through the status items. This is useful if you need to review all of the alarm messages. Press **`ENTER`** again to resume the rotating display.

- **UP/DOWN** displays the previous or next status item.

To access the front panel menu options, press **ESC**. The menu options are as follows:



- **UP/DOWN** navigates to the next menu or submenu item.
- **ENTER** selects a menu or submenu item.
- When you have selected an IP setting from the menu:
  - **UP/DOWN** increases or decreases the value of the currently selected digit.
  - **ENTER** moves the cursor on to the next digit and saves your changes when you move off the final digit.
  - **ESC** cancels any changes; returns to the menu.
- When you are on the **Commands** submenu:
  - **ENTER** performs the command.
  - **ESC** returns to the main menu.
- To leave the menu options and return to the rotating display, press **ESC**.

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: we recommend you 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.
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.

Note that a restart is required for any IP configuration changes to take effect.

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.

Primary LAN 1 IP address

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

In this section of the web page you can configure the primary **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.

Note that the primary LAN 1 IP settings cannot be changed, if this TelePresence Conductor is part of a cluster.

Additional IP addresses for LAN1

When configuring the TelePresence Conductor to work with Unified CM, additional IP addresses must be configured on LAN1 for Ad hoc or rendezvous calls. Up to 64 IP addresses can be added on the **IP** page (**System > IP**). The IP addresses must be in the same subnet as the primary IP address. Each cluster peer must have a unique set of IP addresses.

When the IP addresses have been added, they can be assigned to a Unified CM Location.

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 (FQDN), 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.
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.

We recommend that you 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
- NTP servers
- Remote logging server
- Conference bridges

We recommend that you 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.
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 [p.179] 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.
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 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 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 Cisco 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 Cisco TMS as your external manager, you must select *v3 plus TMS support*.
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.	

Field	Description	Usage tips
Type	The algorithm used to hash 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. If available, the default is and recommended setting 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.

Configuring firewall rules

Firewall rules provide the ability to configure IP table rules to control access to the TelePresence Conductor at the IP level.

The TelePresence Conductor has a set of built-in rules that cannot be modified. The built-in rules can be supplemented by user-configured rules that refine — and typically restrict — what can access the TelePresence Conductor.

Built-in rules

There are two sets of built-in rules that always apply:

- The first set of built-in rules is a single rule that enables the loopback interface. As it is applied before the user-configured rules, it cannot be overridden.
- The second set of built-in rules is applied after the user-configured rules. They enable some specific services and enable access to all traffic destined to this TelePresence Conductor. These rules can be overridden, or refined, by the user-configured rules.

This means that by default everything is allowed access to the TelePresence Conductor. You have to actively configure extra rules to lock down the system to your specifications.

The following table shows the built-in rules, and the sequence in which the built-in and the user-configured rules are applied:

Source address	Destination address	Protocol	Port	Action	Comment
Any	lo	Any	Any	Allow	TelePresence Conductor loopback interface
. . . < user-configured firewall rules are applied here > . . .					
Any	224.0.1.41	UDP	1718	Allow	Multicast address for H.323 gatekeeper discovery
Any	Any	UDP	161	Allow	SNMP traffic
Any	<LAN1 address>	Any	Any	Allow	All traffic for the LAN 1 interface
Any	Any	Any	Any	Deny	Fallback rule to deny traffic not destined for this TelePresence Conductor

The built-in rules and the order in which they are applied cannot be modified.

Note that return traffic from outbound connections is always accepted.

User-configured rules

The user-configured rules are typically used to restrict what can access the TelePresence Conductor. You can:

- specify the source IP address subnet from which to allow or deny traffic
- configure well known services such as SSH, HTTP/HTTPS or specify customized rules based on transport protocols and port ranges
- specify the priority order in which the rules are applied

Setting up and activating firewall rules

The **Firewall rules configuration** page is used to set up and activate a new set of firewall rules.

The set of rules shown will initially be a copy of the current active rules. (On a system where no firewall rules have previously been defined, the list will be empty.) If you have a lot of rules you can use the **Filter** options to limit the set of rules displayed. Note that the built-in rules are not shown in this list.

You can then change the set of firewall rules by adding new rules, or by modifying or deleting any existing rules. Any changes made at this stage to the current active rules are held in a pending state. When you have completed making all the necessary changes you can activate the new rules, replacing the previous set.

To set up and activate new rules:

1. Go to the **Firewall rules configuration** page (**System > Firewall rules > Configuration**).
2. Make your changes by adding new rules, or by modifying or deleting any existing rules as required.
   - New or modified rules are shown as **Pending** (in the **State** column).
   - Deleted rules are shown as **Pending delete**.
3. When you have finished configuring the new set of firewall rules, click **Activate firewall rules**.
4. Confirm that you want to activate the new rules. This will replace the existing set of active rules with the set you have just configured.
   After confirming that you want to activate the new rules, they are validated and any errors reported.
5. If there are no errors, the new rules are temporarily activated and you are taken to the **Firewall rules confirmation** page.
   You now have 15 seconds to confirm that you want to keep the new rules:
   - Click **Accept changes** to permanently apply the rules.
   - If the 15 seconds time limit expires or you click **Rollback changes**, the previous rules are reinstated and you are taken back to the configuration page.

   The automatic rollback mechanism provided by the 15 seconds time limit ensures that the client system that activated the changes is still able to access the system after the new rules have been applied. If the client system is unable to confirm the changes (because it can no longer access the web interface) then the rollback will ensure that its ability to access the system is reinstated.

Rule settings

The configurable options for each rule are:

Field	Description	Usage tips
Priority	The order in which the firewall rules are applied.	The rules with the highest priority (1, then 2, then 3 and so on) are applied first. Firewall rules must have unique priorities. Rule activation will fail if there are multiple rules with the same priority.
IP address and **Prefix length**	These two fields together determine the range of IP addresses to which the rule applies.	The **Address range** field shows the range of IP addresses to which the rule applies, based on the combination of the **IP address** and **Prefix length**. The prefix length range is 0-32 for an IPv4 address.
Service	Choose the service to which the rule applies, or choose *Custom* to specify your own transport type and port ranges.	Note that if the destination port of a service is subsequently reconfigured on the TelePresence Conductor, for example from 80 to 8080, any firewall rules containing the old port number will not be automatically updated.

Field	Description	Usage tips
Transport	The transport protocol to which the rule applies.	Only applies if specifying a *Custom* service.
Start and **end port**	The port range to which the rule applies.	Only applies if specifying a UDP or TCP *Custom* service.
Action	Whether to *Allow* or *Deny* any IP traffic that matches the rule.	For deployments in a secure environment, you may want to configure a set of low priority rules that deny access to all services and then configure higher priority rules that selectively allow access for specific IP addresses.
Description	An optional free-form description of the firewall rule.	If you have a lot of rules you can use the **Filter** by description options to find related sets of rules.

Current active firewall rules

The **Current active firewall rules** page (**System > Firewall rules > Current active rules**) shows the user-configured firewall rules that are currently in place on the system. Note that there is also a set of built-in rules that are not shown in this list.

If you want to change the rules you must go to the **Firewall rules configuration** page from where you can set up and activate a new set of rules.

Managing conference bridges

This section provides information on how to manage conference bridge pools and the conference bridges that are contained in them. It also explains how to change the settings for conference bridges.

About conference bridges 45
Creating conference bridge pools 46
Adding and editing conference bridges 48
Viewing all conference bridges across all pools 52
Moving a conference bridge between pools 53
Adding or editing quality settings 54
Changing global conference bridge settings 55
Conference bridge response time 57

About 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. Conference pools contain conference bridges that are of the same conference bridge type and have identical configuration.

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 Cisco VCS or Unified CM, 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 resources. When using a conference bridge type of TelePresence MCU, it may cascade the conference to other conference bridges in the pool if and when required. If the preferred conference bridge pool cannot be used, the TelePresence Conductor will check the availability of the conference bridges in the pool that is the next highest preference.

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.

The TelePresence Conductor supports up to 2400 concurrent calls. Each cluster of TelePresence Server blades supports a maximum of 104 concurrent calls.

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* and *Cisco TelePresence Servers* 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 resources being used and requested within this conference bridge pool exceeds a given percentage of the total quantity of resources available across all conference bridges in this pool. By default an alarm will be raised when 80% of resources are in use. For more information see Setting the threshold for raising conference bridge resource usage alarms [p.55]
Unified CM location	Contains a list of all Unified CM locations of types *Rendezvous* and *Both* that have been configured on the TelePresence Conductor. A conference bridge pool needs to reference a Unified CM location in order for outbound calls from conference bridges to participants registered on Unified CM to work. Such calls could be initiated by • auto-dialed participants being configured on TelePresence Conductor. • Cisco TMS scheduling a conference with participants. • a user of conference control center in Cisco TMS adding a participant to an existing conference. Use *None* if no outbound calls to participants are required. Change this field after you have created a Unified CM location, if there are no Unified CM locations in the list yet. The **default** is *None*.

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

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

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

Adding and editing conference bridges

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

Before adding a conference bridge, ensure that:

- you configure it in accordance with the relevant deployment guide:
  - *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*, or
  - *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server Deployment Guide*
  - *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server (B2BUA) Deployment Guide*.
- all conference bridges in all pools are configured identically. Failure to do so will result in unpredictable behavior.
- all conference bridges in a pool are of the same conference bridge type.
- all conference bridges used by the TelePresence Conductor are reserved for its exclusive use and are not used by any other system, for example Cisco TelePresence MCU Conference Director.

- all conference bridges in all pools are configured identically. Failure to do so will result in unpredictable behavior.
- all conference bridges in a pool are of the same conference bridge type.
- all conference bridges used by the TelePresence Conductor are reserved for its exclusive use and are not used by any other system, for example Cisco TelePresence MCU 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 that you edit conference bridges at off-peak times.

Note: if you make changes to any of the following options while conferences are in progress on the conference bridge, those conferences will be deleted:

- IP address or FQDN
- Protocol
- Port
- Conference bridge username
- Conference bridge password
- Dial plan prefix
- SIP port

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 **Global conference bridge settings** page (**Conference configuration > Conference bridges > Global conference bridge settings**).

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, when using a Cisco VCS in your deployment, 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. When using the TelePresence Conductor without a valid release key it is only possible to enable one conference bridge across all conference bridge pools. This conference bridge cannot be clustered. If a TelePresence Conductor running without a release key finds more than one conference bridge enabled, for example when a release key existed, but is then deleted, the TelePresence Conductor will set all conference bridges to the *Busied out* state and only leave one conference bridge as *Enabled*. *Enabled*: the conference bridge will be used as and when required. *Busied out*: the conference bridge will not be used for any new conferences.
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*. 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.

Field	Description
Dial plan prefix	(Required when TelePresence Conductor is deployed with Cisco VCS. Not relevant when TelePresence Conductor is deployed with Unified CM.) The prefix that has been configured as part of a Cisco 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. In a Cisco VCS-based deployment, there must not be any conflict between any **Incoming alias** or **Conference name** (used when Creating and editing conference aliases [p.78]), the Call Policy prefix [p.18], and Conference bridge dial plan prefixes [p.18], otherwise you may experience unpredictable behavior. For more information, see Considerations in a Cisco VCS-only deployment [p.18]. For more information on dial plans and prefixes, see Designing a dial plan [p.18]. For more information on Cisco VCS search rule configuration, see *Cisco TelePresence Video Communication Server Administrator Guide*.
Conference bridge type	The type of this conference bridge. This field cannot be modified. This release of the TelePresence Conductor supports *Cisco TelePresence MCUs* and *Cisco TelePresence Servers* 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	(Available when the **Conference bridge pool** has a conference bridge type of *TelePresence MCU*) 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. To see how many content ports your TelePresence MCU model has, see **MCU port matrix** within the Cisco TelePresence MCU online help. The **default** is 0.
SIP port	The port that the conference bridge is listening on for TLS SIP traffic. This is required when Unified CM is being used and when there is a direct SIP trunk from Unified CM to TelePresence Conductor, without going via a VCS. The **default:** is 5061.
H.323 cascade call routing	(Available when the **Conference bridge pool** has a conference bridge type of *TelePresence MCU*) The method used for routing H.323 calls when a conference is cascaded from one conference bridge to another. *Gatekeeper routed*: Calls are routed via an H.323 gatekeeper, for example a Cisco VCS, which the TelePresence Conductor must be registered to. *Direct*: Calls are routed directly from one conference bridge to another without using an H.323 Gatekeeper. The conference bridges must be configured in such a way that IP traffic is routable between them. If you select this setting do not configure an H.323 gatekeeper on the conference bridge, because the setting on the conference bridge will take precedence over this setting and the call will therefore be routed via the conference bridge's H.323 gatekeeper.

Busying out conference bridges

Busying out 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 busied out, 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 in 'Busy out' state, 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 when all existing conferences have been completed.

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

1. Go to the **All conference bridges** page (**Conference configuration > Conference bridges > View all conference bridges**).
2. Select the conference bridge you wish to busy out.
3. Click **Busy out**.

If a TelePresence Conductor is running without a release key and it finds more than one conference bridge enabled, for example when a release key existed, but is then deleted, the TelePresence Conductor will set all conference bridges to the *Busied out* state and only leave one conference bridge as *Enabled*.

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 **All conference bridges** page (**Conference configuration > Conference bridges > View all conference bridges**).
2. Select the conference bridge you wish to delete.
3. Click **Busy out**.
4. Wait until all conferences on that conference bridge have finished (to check, go to **Status > Conference bridges**).
5. Go back to the **All conference bridges** page, select the conference bridge you wish to delete and click **Delete**.

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 click on the conference bridge name or on **View/Edit**.

Moving a conference bridge between pools

To move a conference bridge from one pool to another:

1. Go to the **All conference bridges** page (**Conference configuration > Conference bridges > View all conference bridges**) and 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.
   The conference bridge types of the new pool and the conference bridge being moved have to match.
3. Select **Save**.

Adding or editing quality settings

(This feature is only relevant if using a conference bridge type of TelePresence Server.)

Quality settings consist of an audio quality level and a video quality level. You assign them to conference templates, auto-dialed participants and pre-configured endpoint codecs in order to allow for the required resources to be allocated on the corresponding TelePresence Server.

See Resource reservation and allocation on the TelePresence Server [p.74] for more information on how resources are allocated on a TelePresence Server.

The TelePresence Conductor has been pre-configured with the following quality settings, which can be deleted or edited:

- Full HD (1080p 30fps / 720p 60fps video, multi-channel audio)
- HD (720p 30fps video, stereo audio)
- SD (wide 448p 30fps video, mono audio)

To add a new custom quality setting:

1. Go to the **Quality settings** page (**Conference configuration > Conference bridges > Quality settings**).
2. Click **New**.

When adding or editing a quality setting, the configurable options are:

Field	Description
Description	A free-form description of this quality setting. The descriptions will appear as options in the following drop-down lists: ■ **Participant quality**, **Chairperson quality** and **Guest quality** on the **Conference templates** page ■ **Maximum quality** on the **Auto-dialed participants** page ■ **Quality setting** on the **Codecs** page (accessible when adding codecs to pre-configured endpoints)
Audio quality level	The level of audio quality associated with this quality setting. The options are: ■ Multi-channel ■ Stereo ■ Mono The **default** is *Mono*.
Video quality level	The level of video quality associated with this quality setting. The options are: ■ Full HD (1080p 30fps / 720p 60fps) ■ HD (720p 30fps) ■ SD (wide 448p 30fps) The **default** is *Full HD (1080p 30fps / 720p 60fps)*.

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 resource 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 previously 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 **Conference bridge retry interval** to *0* results in the TelePresence Conductor attempting to contact the conference bridge as often as possible, approximately once every second.

Setting the threshold for raising conference bridge resource usage alarms

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

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

- TelePresence MCU pool exceeds capacity: Unable to create conferences as insufficient TelePresence MCU resource is available in pool
- TelePresence MCUs exceed capacity: Unable to create conferences as insufficient TelePresence MCU resource is available
- TelePresence MCU pool resource warning: TelePresence MCU pool port usage is approaching or has reached full capacity
- TelePresence MCU resource warning: TelePresence MCU port usage is approaching or has reached full capacity
- TelePresence Server pool exceeds device capacity: Unable to create conferences as insufficient TelePresence Server device resource is available in pool
- TelePresence Server pool exceeds license capacity: Unable to create conferences as insufficient

TelePresence Server license resource is available

- TelePresence Servers license capacity exceeded: An individual TelePresence Server's license resource is insufficient to create a conference
- TelePresence Server license resource warning: An individual TelePresence Server's license usage is approaching or has reached full capacity
- TelePresence Server pool license resource warning: TelePresence Server pool license usage is approaching or has reached full capacity
- TelePresence Server device resource warning: An individual TelePresence Server's device 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 resource 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 resources available.
- When a conference could not be created because the number of required resources exceeded the number of resources currently available. The number of required resources for a conference is the total of all auto-dialed participants, reserved chairperson participants, cascade ports, and reserved content resources. 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 resources exceeded the number of resources 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 resource usage drops back below the threshold.

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
- conference bridge under high load
- 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="A conference bridge is taking a long time to respond to requests."
```

Configuring conferences

This section describes the configuration steps required to configure Ad-hoc and Rendezvous conferences on the TelePresence Conductor.

Using the basic conference configuration wizard 59
Selecting the preferred conference bridges for a conference 60
Cascading conferences across conference bridges and conference bridge pools 62
Creating and editing conference templates 63
About resource allocation 73
Limiting the number of participants in a conference 77
Creating and editing conference aliases 78
Creating and editing auto-dialed participants 80
About chairperson and guest roles 87
Creating and editing Unified CM locations 89
Creating and editing pre-configured endpoints 91
Using Call Policy 95

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.

The basic conference configuration wizard only applies in Cisco VCS-based deployments. If configuring the TelePresence Conductor in a Unified CM-based deployment, follow the instructions in the *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.

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 and Cisco VCS according to the instructions in the *Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server Deployment Guide*.

Also 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 Cisco VCS

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.

All bridge pools within a Service Preference must be of the same conference bridge type.

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* and *Cisco TelePresence Servers* 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. When all conference bridge pools have been added and are in the desired order, click **Save**.

You can add more conference bridge pools to a Service Preference later and update the preference order.

Cascading conferences across conference bridges and conference bridge pools

Cascading a conference results in resources being used on a secondary conference bridge when the primary conference bridge does not have enough resources available for all the participants. This release of TelePresence Conductor supports cascading of TelePresence MCUs only. Cascading is not supported on TelePresence Servers.

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.

In a Cisco VCS-based deployment the Cisco VCS acts as an H.323 gatekeeper, via which all calls for conferences that are cascaded from one conference bridge to another are routed.

In a Unified CM-based deployment calls for conferences that are cascaded from one conference bridge to another are routed directly.

Cascading is not supported in Ad hoc conferences, since Ad hoc conferences typically comprise of less than five participants and the overhead of cascading such a small conference would be too large.

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
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. The **default** is *Meeting*.
Number of chairperson participants to reserve	(Available when **Conference type** is *Lecture*) The number of chairperson participants to reserve resources for on the conference bridge. If using TelePresence MCUs, one port per chairperson participant will be reserved on the primary TelePresence MCU. See About resource allocation [p.73] for more information.
Call Policy mode	(Applicable to Cisco VCS deployments) 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 Cisco VCS's Call Policy before allowing users to create a conference. If set to *On*, you must also configure the TelePresence Conductor's Call Policy prefix. See Using Call Policy [p.95] for more information. This should be set to *Off* in a Unified CM - based deployment.
Conference bridge Service Preference	Determines the 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 [p.60].

Field	Description
Number of cascade ports to reserve	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence MCU*) The number of ports to be reserved on the primary TelePresence MCU for connections to additional TelePresence MCUs. These ports will be used if the conference exceeds the capacity of the primary TelePresence MCU and is cascaded to one or more TelePresence MCUs. Each connection between the primary and an additional TelePresence MCU requires one port per conference bridge. 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 Reserving cascade ports [p.73]. For more information about cascading across TelePresence MCUs, see Cascading conferences across conference bridges and conference bridge pools [p.62]
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 other participants (i.e. participants who dial in to the conference, including those who have had chairperson resources reserved). The maximum number of participants must be more than the total number of auto-dialed participants plus the number of reserved chairperson participants. For more information see Limiting the number of participants in a conference [p.77].
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. On a TelePresence Server there will be a warning message displayed as overlaid text on the screen informing you that the conference is about to end. On a TelePresence MCU, depending on the configuration, 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.
Participant quality	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server* and the **Conference type** is *Meeting*) The maximum quality setting to apply to participants using this conference template. Depending on the selected setting the required resources are allocated on the TelePresence Server that is associated with this conference template. The list of available quality settings can be changed on the **Quality settings** page. The pre-configured quality settings are: ■ Full HD (1080p 30fps / 720p 60fps video, multi-channel audio) ■ HD (720p 30fps video, stereo audio) ■ SD (wide 448p 30fps video, mono audio) The **default** is *HD (720p 30fps video, stereo audio)*.

Field	Description
Chairperson quality	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server* and the **Conference type** is *Lecture*) The maximum quality setting to apply to chairpersons using this conference template. Depending on the selected setting the required resources are allocated on the TelePresence Server that is associated with this conference template. The list of available quality settings can be changed on the **Quality settings** page. The pre-configured quality settings are: ■ Full HD (1080p 30fps / 720p 60fps video, multi-channel audio) ■ HD (720p 30fps video, stereo audio) ■ SD (wide 448p 30fps video, mono audio) The **default** is *HD (720p 30fps video, stereo audio)*.
Guest quality	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server* and the **Conference type** is *Lecture*) The maximum quality setting to apply to guests using this conference template. Depending on the selected setting the required resources are allocated on the TelePresence Server that is associated with this conference template. The list of available quality settings can be changed on the **Quality settings** page. The pre-configured quality settings are: ■ Full HD (1080p 30fps / 720p 60fps video, multi-channel audio) ■ HD (720p 30fps video, stereo audio) ■ SD (wide 448p 30fps video, mono audio) The **default** is *HD (720p 30fps video, stereo audio)*.
Provision for multiscreen	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server*) Whether or not the conference will allow provisioning for multiscreen systems. *Yes*: The conference will allow for resources to be made available so that systems with more than one screen can be provisioned. This is also required if pre-configured endpoint checking is required. *No*: The conference will only provision single-screen systems or the primary screen of multiscreen systems. Pre-configured endpoints will not be checked. The **default** is *No*.
Default maximum screens	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server* and when **Provision for multiscreen** is set to *Yes*) The maximum number of screens each endpoint joining the conference is allowed to have. (This setting is only applied to endpoints that have not been pre-configured.) Resources are allocated accordingly on the conference bridge that this conference is hosted on. If **Optimize resources** is set to *Yes* any unused resources are freed up on the conference bridge five seconds after the last person has joined the conference. The **default** is 1. For more information see Allocating resources for multiple screens [p.75].

Field	Description
Optimize resources	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server*) Whether conference bridge resources are optimized for conferences that use this template. *Yes*: Resources that were initially allocated on the conference bridge and that are not being used, are freed up if five seconds pass and no new participant joins the conference. Resources are optimized in the following situations: ■ If there are endpoints in the conference that have an actual number of screens that is lower than the number of **Default maximum screens**. ■ If there are endpoints in the conference that are not using the level of quality defined for the template. *No*: The number of resources consumed by this conference is the same as the number of resources initially allocated on the conference bridge. Some of the resources may be wasted if there are endpoints that have fewer screens than defined or are using a lower quality level than defined. For more information see Optimizing resources [p.76].
Allow content	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence MCU)* 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 MCU and each cascade MCU specifically for content. *No*: participants will not be able to send content, regardless of the number of ports available on the MCU. Content may still be displayed, since some endpoints provide content in their main video channel. The **default** is *Yes*. See Reserving a content port [p.74] for more information.
Content quality	(Available when the **Conference bridge Service Preference** has a conference bridge type of *TelePresence Server*) The video quality level for content, such as presentations, associated with conferences based on this template. The options are: ■ Full HD (1080p 30fps / 720p 60fps) - this setting supports wide UXGA 27fps ■ HD (720p 30fps) ■ 1280 x 720p 15fps ■ 1280 x 720p 5fps ■ Off If *Off* has been selected, there will not be a separate content channel available for conferences based on this template. Content may still be displayed, since some endpoints provide content in their main video channel. The **default** is *Off*. For more information see Allocating resources for content [p.75].

Field	Description
Scheduled conference	Whether or not the conference may only be created by a scheduling application such as Cisco TMS using the API. *Yes*: the conference will be created at a pre-determined time by the scheduling application. Any participants dialing in to the conference before this time will be rejected and will have to call back after the conference has been created. *No*: the conference will be created as soon as the first participant dials in. The **default** is *No*.
Advanced parameters	**Advanced template parameters** are parameters that can be passed to the conference bridge via its API. The parameters can be edited after a conference template has been created. Click **Edit** to get to the **Advanced template parameters** page, where you can select the parameters you would like to send to the conference bridge. See Adding and editing advanced template parameters [p.67] for more information. **CAUTION**: this feature is for advanced use only.

Adding and editing advanced template parameters

CAUTION: this feature is for advanced use only.

Cisco TelePresence MCUs support the *Cisco TelePresence MCU Remote Management API* and Cisco TelePresence Servers support the *Cisco TelePresence Server API*. These APIs enable third-party control of the relevant conference bridge via messages sent using the XML-RPC protocol. The TelePresence Conductor uses these APIs to manage conferences on the conference bridges in its pool. It supports the TelePresence MCU's API versions 2.8 and 2.9 and the TelePresence Server's API version 3.0.

The TelePresence Conductor allows you to make use of the calls `conference.create` (for TelePresence MCU) and `flex.conference.create` (for TelePresence Server) of these APIs through the **Advanced template parameters** page. This page is accessible via the **Conference templates** page (**Conference configuration > Conference templates**) when a conference template has been created.

When a conference is created on a conference bridge, the settings for that conference will depend on the conference bridge template being used. However, settings configured via the **Advanced template parameters** on the TelePresence Conductor will override any settings specified by the template on the conference bridge.

To create or edit advanced template parameter settings:

1. Create a new conference template or select an existing conference template (**Conference configuration > Conference templates**)
2. In the **Advanced parameters** section click **Edit**.
   The **Advanced template parameters** page
3. Select the check-boxes next to all the parameters that should be sent to the conference bridge.
   For TelePresence MCU there are two check-boxes: the first one for the primary TelePresence MCU and the second one for the cascade TelePresence MCU.
4. Enter or select the relevant parameter values.

Cisco TelePresence MCU parameters

Note: all TelePresence MCUs should be running the same release of software in order to guarantee consistent availability and behavior of the various parameters.

The configurable options for TelePresence MCUs are:

Field name	Parameter in API	Description
Automatic lecture mode	`automaticLectureMode`	Automatic lecture mode allows the lecturer (chair) to be shown in full-screen view to the students. In this mode, the lecturer will continue to see their normal (continuous presence) view. That is, the lecturer will see the students (guests) and not himself. The TelePresence MCU identifies the lecturer and controls the layout seen by the other participant according to which mode is selected here. *Type 1*: The speaker sees continuous presence (or their custom layout) and all participants see the guest who is speaking (be they a chair or a guest). *Type 2*: All guests, including the speaker, see the last chair who spoke full screen. All chairs will see their custom layout. *Disabled*: Automatic lecture mode is disabled."
Timeout for automatic lecture mode type 1	`automaticLectureModeTimeout`	This parameter is applicable if an **Automatic lecture mode** of *Type 1* is selected. The value (in seconds) determines how quickly the loudest speaker will appear in full-screen view to the other participants.
Floor and chair control	`chairControl`	Controls floor and chair control settings for this conference. *None*: the use of floor and chair controls is not allowed in this conference. *Floor control only*: only floor control is allowed in this conference; chair control is not allowed. Any participant can 'take the floor' so long as no other participant has currently 'taken the floor'. *Chair and floor control*: both chair and floor control are allowed in this conference. Any participant can 'take the floor' and any chairperson participant can 'take the chair' so long as no other participant has currently done so. *Default*: use the default setting on the TelePresence MCU. See the relevant TelePresence MCU's Online Help for more information on **Floor and chair control**.

Field name	Parameter in API	Description
Content mode	`contentMode`	Defines the content mode of the conference. Do not use when running TelePresence MCU version 4.2. *Transcoded*: content is always transcoded. The TelePresence MCU sends out a single, transcoded content stream. *Pass-through*: content is not decoded and is simply repackaged and sent out to each eligible endpoint in the conference. *Hybrid*: The TelePresence MCU sends out two content streams: a passed-through higher resolution stream, and a lower resolution stream transcoded and scaled down for any endpoints that are unable to support the higher stream.
Transmitted content resolutions	`contentTransmitResolutions`	The resolution for the content channel that will be transmitted to endpoints in conferences based on this template. *4-to-3 only*: the TelePresence MCU encodes the content and transmits it in a resolution of ratio 4:3. *16-to-9 only*: the TelePresence MCU encodes the content and transmits it in a resolution of ratio 16:9. *Allow all*: the TelePresence MCU decides on the most optimal resolution depending on information about capabilities sent by the endpoints in the conference.
Outgoing transcoded codec	`contentTxCodec`	The codec used to transmit content in conferences based on this template. If content is to be transcoded, this is the output format of the transcoder: *H.263+* or *H.264*. This setting does not apply in *Pass-through* mode.
Minimum bit rate to use for transmitted content	`contentTxMinimumBitRate`	Sets a lower limit on the bandwidth of the shared content video encoding sent to content receivers in a conference. Measured in bps.
Custom layout enabled	`customLayoutEnabled`	Whether a custom layout can be used for all participants in conferences based on this template. To use custom layouts, the field **New participants will see custom layout** must be set to *True* and **Custom layout** must be set to the appropriate value.
Custom layout	`customLayout`	The index number of the video layout seen by the conference participants. See Conference layouts [p.170] for a list of available layouts and corresponding index values. To use custom layouts, the fields **New participants will see custom layout** and **Custom layout enabled** must both be set to *True*.
Description	`description`	Additional information about the conference.

Field name	Parameter in API	Description
Encryption required	`encryptionRequired`	The encryption setting for conferences based on this template. If *True*, encryption is required for these conferences; otherwise, encryption is optional. If encryption is required, the TelePresence MCU must have the encryption feature key enabled.
Guest PIN	`guestPin`	If a conference has a **Guest PIN** set, guest participants cannot join the conference or change its configuration without entering the correct PIN.
Audio muted initially	`joinAudioMuted`	Whether to initially mute audio from all participants when they join the conference.
Video muted initially	`joinVideoMuted`	Whether to initially turn video off from all participants when they join the conference.
Disconnect when last chairperson leaves	`lastChairmanLeavesDisconnect`	Whether all other participants will be disconnected when the last participant with chairperson status leaves the conference.
Layout control via FECC/DTMF	`layoutControlEx`	Defines how the view layout can be controlled. The setting can be overridden in an endpoint's individual configuration. *Disabled*: participants are not allowed to change their view layout using either far end camera control (FECC) or dual-tone multi frequency (DTMF). *FECC only*: participants can only change their view layout using FECC. *DTMF only*: participants can only change their view layout using DTMF. *FECC with DTMF fallback*: participants can change their view layout using FECC when it is available and via DTMF on endpoints, which do not have FECC. *Both FECC and DTMF*: participants can change their view layout using both FECC and DTMF.
New participants will see custom layout	`newParticipantsCustomLayout`	Whether new participants use the custom layout or not. To use custom layouts, the field **Custom layout enabled** must be set to *True* and **Custom layout** must be set to the appropriate value.
PIN	`pin`	If a conference has a **PIN** set, chairperson participants cannot join the conference or change its configuration without entering the correct PIN.
Mute in-band DTMF	`suppressDtmfEx`	Controls the muting of in-band dual-tone multi-frequency (DTMF) tones. *FECC*: in-band DTMF tones will be muted when DTMF is being used to control layout because far end camera control (FECC) is not available. *Always*: in-band DTMF tones will always be muted. *Never*: in-band DTMF tones will never be muted.

Field name	Parameter in API	Description
Template number	`templateNumber`	An index that uniquely identifies the TelePresence MCU template.
Template name	`templateName`	The name of the TelePresence MCU template.
Custom parameters		This field can be used to enter advanced parameters and their corresponding values in valid JSON. 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 TelePresence 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 TelePresence MCU becoming temporarily unusable and excluded from the pool of available conference bridges.

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

Cisco TelePresence Server parameters

The configurable options for TelePresence Servers are:

Field name	Parameter in API	Description
Guest PIN	`guestPin`	If a conference has a Guest PIN set, guest participants cannot join the conference or change its configuration without entering the correct Guest PIN.
PIN	`pin`	If a conference has a PIN set, chairperson participants cannot join the conference or change its configuration without entering the correct PIN.
Single-screen layout	`displayDefaultLayoutSingleScreen`	The default layout type on single-screen endpoints using this conference template. This setting can be overridden by a participant using far end camera control (FECC) or dual-tone multi-frequency (DTMF) keys when in the conference. *Single*: the active speaker is shown in one full-screen pane. *ActivePresence*: the active speaker is shown in a large pane with additional participants appearing in up to nine PIPs (picture-in-pictures) overlaid at the bottom of the screen. *Prominent*: the active speaker is shown in a large pane with additional participants appearing in up to four smaller panes at the bottom of the screen. *Equal*: conference participants are shown in a grid pattern of equal sized panes, up to 4x4.
Multiscreen layout	`displayDefaultLayoutMultiScreen`	The default layout type on multiscreen endpoints using this conference template. This setting can be overridden by a participant using far end camera control (FECC) or dual-tone multi-frequency (DTMF) keys when in the conference. *Single*: all screens of the endpoint with the active speaker are shown full-screen on the multiscreen endpoint. *ActivePresence*: all screens of the endpoint with the active speaker are shown full-screen on the multiscreen endpoint, additional participants appear in up to nine PIPs (picture-in-pictures) overlaid at the bottom of the screen.
Custom parameters		This field can be used to enter advanced parameters and their corresponding values in valid JSON. For more information on the parameters that can be configured see Cisco TelePresence Server API 3.0 Reference Guide.

About resource allocation

Each conference is hosted on one or more conference bridges. 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 resources that conference will require, so it can assign the conference to a conference bridge that has sufficient resources.

Resource reservation and allocation on the TelePresence MCU

The TelePresence MCU uses the concept of ports to allocate resources. One TelePresence MCU port is allocated for each conference participant, not differentiating between quality levels.

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 TelePresence MCUs, which should be set to *Disabled*.

Reserving chairperson participants

A Lecture-type conference can have more than one chairperson. Each chairperson requires conference bridge resources to send and receive audio and video. Resources will be allocated on the primary conference bridge if available; if there is no resource available on the primary conference bridge, and if the template is configured to support cascades, the resources will be made available on a cascade conference bridge. If the chairperson is allocated resources on a cascade conference bridge, they will not have all the capabilities that they would if they were on the primary conference bridge (for example, layout experience and control functionality may not behave as expected).

We therefore recommend that you enter a **Number of chairperson participants to reserve** that is equal to the number of chairpersons. This will reserve resource on the primary conference bridge for all chairpersons, so that they all get the same experience.

Reserved chairperson resources are reserved for the duration of the conference, and are reserved solely for the use of chairpersons of this conference.

By default guests dialing into a Lecture-type conference before the Chairperson will be kept holding on an entry screen.

Reserving 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 can 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 reserved cascade port on the primary conference bridge and one port on the cascade conference bridge. To reserve the required number of cascade ports on the primary conference bridge specify the **Number of cascade ports to reserve** when creating a conference template on the TelePresence Conductor. 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.

Reserving a content port

Conference participants may want to send content video such as a presentation. Such content requires 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, if the conference cascades, a port on each cascade conference bridge specifically for content. Any participant can receive content from these ports, but only one participant at a time can send content.

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. Content will only be displayed if the endpoint provides content in its main video channel.

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

Allocating ports

On the TelePresence MCUs one port is allocated for each participant joining a conference. Ports can be reserved for chairpersons and to allow cascading to additional TelePresence MCUs.

Some TelePresence MCUs have dedicated content and audio ports. When reserving or allocating resources for content the dedicated content ports are used first, and when all have been used, normal video ports are used for content. The TelePresence Conductor does not make use of the dedicated audio ports. It assumes that all participants require video at some point and allocates video ports for both video and audio-only calls.

Resource reservation and allocation on the TelePresence Server

The TelePresence Server allocates resources based on the required audio, video and content quality level for a conference. The Quality settings page on TelePresence Conductor allows you to edit the pre-configured quality settings or define new quality settings.

Reserving chairperson participants

A Lecture-type conference can have more than one chairperson. There must be sufficient resources available on one single conference bridge for all chairpersons to join the conference. To ensure that there are enough resources available for all chairpersons to join the conference, when creating a conference template you are asked how many chairperson participants the TelePresence Conductor should reserve on the conference bridge.

The **Number of chairperson participants to reserve** is multiplied by the number of resources that are required for the **Chairperson quality** defined on the same template:

Total amount of resources reserved = Number of chairperson participants to reserve * (Chairperson quality + Content quality)

The appropriate number of resources are reserved for the duration of the conference, solely for the use of chairpersons.

If the conference requires more chairperson resources than have been reserved, a chairperson may still be able to connect to the conference but only if the conference bridge hosting the conference has sufficient resources available.

Allocating resources for participants and guests

Resources for participants in Meeting-type conferences and for guests in Lecture-type conferences are allocated as required when a participant joins a conference.

The number of resources that must be allocated for each participant depends on the quality settings for audio and video. These are defined for the conference template using **Participant quality** and **Guest quality**.

Allocating resources for content

Conference participants may want to send content video such as a presentation. Such content requires separate resources to be allocated on the conference bridge.

The number of resources to allocate on the conference bridge is determined by the **Content quality** setting on the conference template.

The table below shows the proportions of resources allocated for each pre-configured content quality setting.

Content quality setting	Proportions of resources allocated
Full HD (1080p 30fps / 720p 60 fps)	
HD (720p 30fps)	0.5 of the resources for Full HD (1080p 30fps / 720p 60fps)
1280 x 720p 15fps	0.5 of the resources for HD (720p 30fps)
1280 x 720p 5fps	0.33 of the resources for 1280 x 720p 15fps
Off	None

If you have selected *Off*, participants will **not** be able to send content, regardless of the number of resources available on the conference bridge. Content will only be displayed if the endpoint provides content in its main video channel.

Allocating resources for multiple screens

For TelePresence Server to support multiscreen endpoints you must:

- set **Provision for multiscreen** to *Yes* on the conference template
- either:
  - pre-configure all multiscreen endpoints on the Pre-configured endpoint page (this is essential for custom multiscreen endpoints), or
  - set the **Default maximum screens** on the conference template to the largest number of screens that should be supported in the conference (possible for TIP negotiated multiscreen endpoints such as CTS, and for T3)

For optimal resource usage, we recommend that you pre-configure multiscreen endpoints and set the **Default maximum screens** to *1*.

Allocating resources for pre-configured custom endpoints

For pre-configured custom endpoints the number of resources that are allocated on the conference bridge is based on the quality settings for all codecs.

For example, if two custom endpoints, each with three screens/codecs, have been pre-configured, the resources required for the quality settings of each of the six codecs are added up.

Allocating resources for pre-configured TIP negotiated multiscreen endpoints and for T3

For pre-configured TIP negotiated multiscreen endpoints, such as CTS, and for T3, the number of resources are based on the quality setting for the codec that has been defined, multiplied by three for the number of screens.

For example, if two CTSs have been pre-configured, the resources required for the quality settings of each codec are multiplied by three and then added together.

Allocating resources for TIP negotiated multiscreen endpoints that have not been pre-configured

If **Default maximum screens** is set on the conference template, the conference bridge allocates the appropriate resources based on the quality setting for each chairperson, participant or guest joining the conference, multiplied by the **Default maximum screens**.

For example, if the **Default maximum screens** is set to 3, all participants joining the conference are initially assumed to have three screens.

Optimizing resources

If **Optimize resources** is set for the template, resources that were initially allocated for a particular conference on the TelePresence Server, but that are not being used, are freed up.

Resource optimization does not happen immediately when a call arrives in a conference - it leaves a short while for the resource negotiations to stabilize.

The TelePresence Conductor has to assume that any caller joining a conference will use the maximum resources available to it, as determined by the conference template used to create the conference. When the endpoint is in the conference and the conference is stable the TelePresence Conductor can optimize its view of the conference – taking into account the actual resource each endpoint is capable of using, based on the codec negotiations that the endpoint has made with the conference bridge.

Resource optimization is performed in the following way:

1. Per-caller optimization is performed 5 seconds after the latest attendee joined the conference.
2. Callers who leave the conference will have all their resources returned 30 seconds after the latest attendee joined the conference.

Resources are not optimized for auto-dialed participants and pre-configured endpoints.

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), participants for which resources have been reserved (i.e. chairperson participants), plus all other participants (i.e. participants who dial in to the conference using one of the conference aliases). The number of participants does not include any resources 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 resources have been reserved (i.e. the setting in the **No. of chairperson participants 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 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 dial-in participant, plus all auto-dialed and reserved chairperson participants, plus any additional 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 participants is equal to or higher than the maximum
- the number of reserved chairperson participants is changed, and doing so means that the number of auto-dialed participants plus reserved chairperson participants 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 participants.

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).

Conference aliases are required for all rendezvous conferences in Cisco VCS and Unified CM deployments.

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.

There must not be any conflict between any **Incoming alias** or **Conference name**.

In a Cisco VCS-based deployment, there must not be any conflict between any **Incoming alias** or **Conference name**, the Call Policy prefix [p.18], and Conference bridge dial plan prefixes [p.18], otherwise you may experience unpredictable behavior. For more information, see Considerations in a Cisco VCS-only deployment [p.18].

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, see About regular expressions [p.162].
- For specific examples of how regular expressions can be used to set up conference aliases see Regular expression examples - conference aliases [p.163] and Regular expression examples - Lectures [p.166].

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	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 [p.79] for more information.

Field	Description
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 0) 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 types** will be available in the following field.
Role type	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 [p.87] for more information on the differences between the two roles.

Conference name length

TelePresence MCUs support conference names of up to 31 characters and TelePresence Servers support conference names of up to 150 characters. If the TelePresence Conductor has a conference name that is longer than the maximum number of supported characters it will hash the name and pass the hash value to the conference bridge for it to use as the conference name. The TelePresence Conductor will continue to use the original name itself.

If a conference name is longer than 31 (for TelePresence MCU) or 150 (for TelePresence Server) characters, you can view the hashed value on the **Conferences status** page (**Status > Conferences**):

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

To avoid hashing, we recommend that you use conference names that are 31 characters or fewer for TelePresence MCUs and 150 characters or fewer for TelePresence Servers. 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. For information on how to test your dial plan see Check dial plan [p.140].

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.

This release of the TelePresence Conductor does not support auto-dialed participants that are multiscreen endpoints.

Each auto-dialed participant is associated with a **Conference template** and has a **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 match 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 for conference creation, 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)	A filter defining which conferences this participant will be added to. 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**. The default regular expression needs to be used for auto-dialed participants in Unified CM Ad hoc conferences, because all conference names are unique and generated by the Unified CM.
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*. If this auto-dialed participant will be used with Unified CM, *SIP* must be selected.

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 participant will join the conference as a chairperson. *Chairperson* (available when the template **Type** is *Lecture*): the participant will join the conference as a chairperson. *Guest* (available when the template **Type** is *Lecture*): the participant will join the conference as a guest. For more information on the differences between the two roles for a Lecture, see About chairperson and guest roles [p.87]
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 [p.82].
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*.
Maximum quality	(Available when the **Conference template** has a conference bridge type of *TelePresence Server*) The maximum quality setting to apply to this auto-dialed participant. Depending on the selected setting the required resources are allocated on the TelePresence Server that is associated with this auto-dialed participant. The quality settings can be changed on the **Quality settings** page. The initial list of quality settings includes: ■ Full HD (1080p 30fps / 720p 60fps video, multi-channel audio) ■ HD (720p 30fps video, stereo audio) ■ SD (wide 448p 30fps video, mono audio)
State	If *Enabled*, calls will be made to this auto-dialed participant when a conference is created using the selected template. If *Disabled*, the auto-dialed participant is ignored.

Field	Description
Advanced parameters	**Advanced parameters** are parameters that can be passed to the conference bridge hosting the conference this auto-dialed participant is configured for, via its API. The parameters can be edited after an auto-dialed participant has been created. Click **Edit** to get to the **Advanced auto-dialed participant parameters** page, where you can select the parameters you would like to send to the conference bridge. This release of TelePresence Conductor only supports advanced auto-dialed participant parameters for TelePresence MCUs, not for TelePresence Servers. See Adding and editing advanced auto-dialed participant parameters [p.83] for more information. **CAUTION**: this feature is for advanced use only.

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 must 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 cannot 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 the TelePresence MCU does in such situations by going to its **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.

Adding and editing advanced auto-dialed participant parameters

CAUTION: this feature is for advanced use only.

This release of TelePresence Conductor only supports advanced auto-dialed participant parameters for TelePresence MCUs. It does not support them for TelePresence Servers.

Advanced auto-dialed participant parameters are parameters that can be configured for an auto-dialed participant and passed via its API to the conference bridge that hosts the conference this auto-dialed participant is associated with.

The parameters are selected on the **Advanced auto-dialed participant parameters** page, which is accessible via the **Auto-dialed participants** page (**Conference configuration > Auto-dialed participants**, then click **Edit** in the **Advanced parameters** section), when an auto-dialed participant has been created.

Advanced parameters for auto-dialed participants are configured and passed on in a similar way to advanced template parameters.

To create or edit advanced auto-dialed participant parameter settings:

1. Create a new auto-dialed participant or select an existing auto-dialed participant (**Conference configuration > Auto-dialed participants**).
2. In the **Advanced parameters** section click **Edit**.
   The **Advanced auto-dialed participant parameters** page will open.
3. Select the check-boxes next to all the parameters that should be sent to the conference bridge.
4. Enter or select the relevant parameter values.

Cisco TelePresence MCU parameters

The configurable options for TelePresence MCUs are:

Field name	Parameter in API	Description
Appear as a recording device	`actAsRecorder`	Whether this participant appears as a recording device to other participants.
Apply fixed gain	`audioRxGainMillidB`	If **Adaptive gain control** is *Fixed*, this is the gain applied, in millidB. It can be a negative value.

Field name	Parameter in API	Description
Adaptive gain control	`audioRxGainMode`	Whether and how audio gain is applied. Choose from: *None*: no extra gain is applied. *Automatic*: automatic gain control is applied. *Fixed*: a fixed number of millidBs of gain is applied.
Audio muted initially	`audioRxMuted`	Whether audio from this participant will be muted, so that this participant cannot be heard by other conference participants.
View border size	`borderWidth`	Controls the width of the outer border of the auto-dialed participant's layout. *0* indicates that there is no outer border added. *1*, *2* and *3* indicate that borders are added matching the width defined for these values on the TelePresence MCU. *3* is the widest.
Custom layout	`cpLayout`	The type of video layout seen by the conference participants. See Conference layouts [p.170] for a list of available layouts.
Display name override status	`displayNameOverrideStatus`	Whether the participant uses the **Display name override value** to identify itself.
Display name override value	`displayNameOverrideValue`	If **Display name override mode** is *true*, this value overrides the participant's display name.
H.323 gateway address	`gatewayAddress`	The address of an H.323 gateway, if required. Only applicable if the auto-dialed participant's **Protocol** is *H.323*.
Content negotiation	`h239Negotiation`	Defines how the TelePresence MCU presents itself for H.239 token negotiation. *As master*: the TelePresence MCU acts as master in H.239 token negotiation. *As slave*: the TelePresence MCU acts as the slave in H.239 token negotiation and can send content to a master unit if it accepts the token request. *Mimic slave*: the TelePresence MCU acts as a mimic slave in H.239 token negotiation and will try to send content to all other endpoints/units even if this unit (i.e. the mimic slave) rejects the token request.

Field name	Parameter in API	Description
Layout control via FECC/DTMF	`layoutControlEx`	Defines how the video layout can be controlled for this auto-dialed participant. *Disabled*: layout control is disabled. *FECC only*: the auto-dialed participant can only change the view layout using far end camera control (FECC). *DTMF only*: the auto-dialed participant can only change the view layout using dual-tone multi-frequency (DTMF). *FECC with DTMF fallback*: the auto-dialed participant can change the view layout using FECC when it is available and via DTMF , when FECC is not available. *Both FECC and DTMF*: the auto-dialed participant can change the view layout using both FECC and DTMF.
Link type	`linkType`	Defines the type of auto-dialed participant. *Default*: the auto-dialed participant is an endpoint or recording device that is called into the conference. *Cascade slave to master*: the auto-dialed participant is a cascaded conference bridge that is called into a conference. This option allows for participants connected to a particular conference bridge to be joined into a conference that is hosted on another (master) conference bridge and for both to appear as one large conference bridge.
Preferred bandwidth from MCU	`maxBitRateFromMCU`	Maximum bandwidth from the TelePresence MCU in kbps.
Preferred bandwidth to MCU	`maxBitRateToMCU`	Maximum bandwidth to the TelePresence MCU in kbps.
Motion/sharpness tradeoff	`motionSharpnessTradeoff`	Defines the preference for motion versus sharpness. The options are: *Default*: use the global default setting. *Prefer motion*: prefer motion at the expense of sharpness. *Prefer sharpness*: prefer sharpness at the expense of motion. *Balanced*: balance the motion and sharpness trade-off.
Password	`password`	The password the TelePresence MCU uses to access VNC endpoints.
Mute in-band DTMF	`suppressDtmfEx`	Controls the muting of in-band dual-tone multi-frequency (DTMF) tones. *FECC*: in-band DTMF tones will be muted when DTMF is being used to control layout because far end camera control (FECC) is not available. *Always*: in-band DTMF tones will always be muted. *Never*: in-band DTMF tones will never be muted.

Field name	Parameter in API	Description
Transport protocol	`transportProtocol`	Defines the SIP transport protocol. Only applicable if the auto-dialed participant's **Protocol** is *SIP*. One of Default, TCP, UDP or TLS. Default is the default transport protocol configured on the TelePresence MCU.
Use SIP registrar	`useSIPRegistrar`	Whether the auto-dialed participant uses the SIP registrar. Only applicable if the auto-dialed participant's **Protocol** is *SIP*.
Received video resolutions	`videoRxMaxResolution`	The maximum resolution of the received video. The options are: *CIF*: this participant sends CIF or lower resolution to the TelePresence MCU. *4CIF*: this participant sends 4CIF or lower resolution to the TelePresence MCU. *Maximum*: this participant sends the maximum resolution that both sides can support.
Video muted initially	`videoRxMuted`	Whether video from this participant is muted and the participant cannot be seen by other conference participants.
Transmitted video resolutions	`videoTxMaxResolution`	The maximum resolution of the transmitted video. The options are: *CIF*: the TelePresence MCU sends CIF or lower resolution to this participant. *4CIF*: the TelePresence MCU sends 4CIF or lower resolution to this participant. *Maximum*: the TelePresence MCU sends the maximum resolution that both sides can support.
Transmit widescreen video	`videoTxWidescreen`	Whether the TelePresence MCU sends video in a form suitable for a widescreen 16:9 display to this participant.
Custom parameters		This field can be used to enter advanced parameters and their corresponding values in valid JSON. The TelePresence Conductor does not perform in-depth checking of data in these fields. Any incorrect configuration of the settings may result in your auto-dialed participant failing to be called into the conference.

Cisco TelePresence Server parameters

This release of TelePresence Conductor only supports advanced auto-dialed participant parameters for TelePresence MCUs. It does not support them for TelePresence Servers.

About chairperson and guest roles

Conference bridges have two types of conference participant: **Chairperson** and **Guest**. Lecture-type conferences can have more than one chairperson and more than one guest. Meeting-type conferences can only have one type of participant, so all Meeting participants are given a role of 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 [p.78] 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 [p.80] for more information.

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. On a TelePresence MCU 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 TelePresence MCU.

This setting can be modified via the advanced template parameter **Disconnect when last chairperson leaves** on the TelePresence Conductor under **Conference configuration > Conference template > Advanced parameters**.

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 TelePresence MCU parameter **Disconnect when last chairperson leaves** 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 Adding and editing advanced template parameters [p.67].

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 TelePresence 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 TelePresence 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*.

Creating and editing Unified CM locations

TelePresence Conductor supports conferences between endpoints registered directly with Unified CM version 8.6.2 or later. A Unified CM location is needed to mimic the Unified CM's expectation that it is connecting to separate conference bridges in different locations. Both Ad hoc conferences and Rendezvous conferences are supported.

A Unified CM location is also required when the TelePresence Conductor is directly connected to one or more Cisco VCS(s) via the B2BUA. One Unified CM location is used for all Cisco VCSs (or Cisco VCS clusters), which the TelePresence Conductor is connected to.

To create a new Unified CM location:

1. Go to the **Unified CM locations** page (**Conference configuration > Unified CM locations**.
2. Click **New**.

When creating or editing a Unified CM location, the configurable options are:

Field	Description
Location name	A descriptive name of the Unified CM location.
Description	A free-form description of the Unified CM location.
Conference type	Determines the type of Unified CM conference supported by this Unified CM location. *Ad hoc*: A non-scheduled, spontaneous meeting where a user brings two or more people together in a conference that has not been pre-planned. The conference is initiated by using the conference button on the endpoint. *Rendezvous*: A non-scheduled conference for which the host knows the conference dial-in beforehand and must share it with all participants. *Both*: Ad hoc and rendezvous conferences. This needs to be selected when outbound calls, for example to auto-dialed participants, are required for Ad hoc conferences. See Adding auto-dialed participants to Unified CM for Ad hoc conferences [p.90].
Ad hoc IP address (local)	(Only applicable to Ad hoc conferences) The IP address on TelePresence Conductor used for Ad hoc conferences associated with this Unified CM location. The Unified CM is configured to use this IP address to send Ad hoc conference requests to the TelePresence Conductor. The drop-down list contains IP addresses already configured for this TelePresence Conductor, but not yet assigned to a Unified CM location. If there are no IP addresses in the list, go to the **IP** page (**System > IP**) to add more IP addresses to the TelePresence Conductor. Each cluster peer must be configured individually, as the IP address is unique per peer.
Template	(Only applicable to Ad hoc conferences) The conference template to use for Ad hoc conferences associated with this Unified CM location. Only Meeting-type templates are displayed in the drop-down box.

Field	Description
Rendezvous IP address (local)	(Applicable to rendezvous conferences and Ad hoc conferences where outbound calls may be used, for example to auto-dialed participants) The IP address on the TelePresence Conductor used for rendezvous conferences. The Unified CM is configured with a SIP trunk that uses this IP address to send rendezvous calls to the TelePresence Conductor. For outbound calls, for example to auto-dialed participants, in both rendezvous and Ad hoc conferences, this is the source IP address for the connection to the Unified CM. The drop-down list contains IP addresses already configured for this TelePresence Conductor, but not yet assigned to a Unified CM location. If there are no IP addresses in the list, go to the **IP** page (**System > IP**) to add more IP addresses to the TelePresence Conductor. Each cluster peer must be configured individually, as the IP address is unique per peer.
Trunk IP address	(Only applicable to conferences that have out-dial participants) The IP address of the Unified CM that hosts the SIP trunk for outbound calls within rendezvous and Ad hoc conferences. The trunk IP address is required if: ■ there are auto-dialed participants configured on the TelePresence Conductor. ■ Cisco TMS schedules a conference with participants. ■ a user of conference control center (CCC) in Cisco TMS adds a participant to an existing conference.
Trunk port	(Only applicable to conferences that have out-dial participants) The port number for the SIP trunk for outbound calls within rendezvous and Ad hoc conferences. The **default** is *5061*.
Trunk transport protocol	(Only applicable to conferences that have out-dial participants) The transport protocol for the SIP trunk for outbound calls within rendezvous and Ad hoc conferences. The options are either *TLS* or *TCP*. The **default** is *TLS*.

Adding auto-dialed participants to Unified CM for Ad hoc conferences

When adding auto-dialed participants to Unified CM for use with Ad hoc conferences it is important to follow these steps:

1. On the **IP** page (**System > IP**) add local IP addresses to the TelePresence Conductor for the Ad hoc conferences and for outbound calls (entered into the **Rendezvous IP address (local)** field).
2. On the **Unified CM locations** page (**Conference configuration > Unified CM locations**) set the Unified CM location's **Conference type** field to *Both* and set all required fields.
   The **Rendezvous IP address (local)** is the source IP address on the TelePresence Conductor that is used for outbound calls. The **Trunk settings** are the settings on the Unified CM that are used for outbound calls.
3. On the **Conference bridge pools** page (**Conference configuration > Conference bridges > Conference bridge pools**) select the conference bridge pool that is used for this Ad hoc conference and set the **Unified CM location** that was created in the previous step.

Creating and editing pre-configured endpoints

If your deployment includes any multiscreen endpoints we recommend that you pre-configure these on the TelePresence Conductor. This will ensure that appropriate resources are allocated on the TelePresence Servers that host the conferences the multiscreen endpoints dial into. Pre-configuring endpoints involves creating a pre-configured endpoint and then adding between one and four codecs to it. Single-screen endpoints can also be pre-configured.

TelePresence MCUs do not support multiscreen endpoints.

The TelePresence Conductor supports endpoints with more than one screen, provided the conferences they dial into are hosted on a TelePresence Server and the field **Provision for multiscreen** has been set to *Yes* on the **Conference templates** page. Supported endpoints are:

- Cisco TelePresence System T3 (T3) and Multiscreen TIP endpoints, e.g. Cisco TelePresence System series (CTS)
  It is optional to pre-configure these endpoints. For more information see Allocating resources for multiple screens [p.75].
- Custom endpoints, which are all other multiscreen endpoints that are compatible with TelePresence Server version 3.0 and have up to four codecs
  These endpoints **have** to be pre-configured, otherwise only the codec that is dialing into the conference will have its associated screen displayed.

Conference templates used by T3 and Telepresence Interoperability Protocol (TIP) negotiated multiscreen endpoints, such as CTS, must not have **Content quality** set to *Off*. The templates must have at least a **Content quality** setting of *1280 x 720p 5fps* for the endpoints using the templates to be seen as multiscreen endpoints.

To create a new pre-configured endpoint:

1. Go to the **Pre-configured endpoints** page (**Conference configuration > Pre-configured endpoints**.
2. Click **New**.

When creating or editing a pre-configured endpoint, the configurable options are:

Field	Description
Name	A descriptive name of the endpoint.
Description	A free-form description of the endpoint.
Endpoint type	The type of endpoint to pre-configure. *Custom*: any endpoints that have more than one codec *Multiscreen TIP endpoint and T3*: multiscreen endpoints that are compliant with the Telepresence Interoperability Protocol, such as Cisco TelePresence System series, and Cisco TelePresence System T3 endpoints. For these endpoints to be treated as a multiscreen endpoint the associated conference template must have a **Content quality** of at least *1280 x 720p 5fps*. Only the details of the primary codec need to be pre-configured. **Note:** when configuring multiscreen endpoints you must also enable **Provision for multiscreen** on all conference templates that are to check for pre-configured endpoints.

Field	Description
State	Whether or not the pre-configured endpoint is enabled. When the pre-configured endpoint is *Disabled*, the endpoint can still dial into a conference, but resources are not allocated for it and it is seen as a single-screen endpoint. The **default** is *Enabled*.
Display name	Name to display in conference (in preference to endpoint URI) if endpoint name display is enabled on the conference bridge.
Receiver audio gain	Volume adjustment for incoming audio (used to adjust loudspeaker volume across codecs). *0* means that there is no change in volume of incoming audio. Negative values indicate a lower volume and positive values indicate a higher volume. Values are in dBm.
Transmitter audio gain	Volume adjustment for outgoing audio (used to adjust loudspeaker volume across codecs). *0* means that there is no change in volume of outgoing audio. Negative values indicate a lower volume and positive values indicate a higher volume. Values are in dBm.
Initial outgoing audio	When initially joining a conference the endpoint audio may be muted or active. The **default** is *Active*.
Initial incoming audio	When initially joining a conference the received audio may be muted or active. The **default** is *Active*.
Initial outgoing video	When initially joining a conference the endpoint video may be muted or active. The **default** is *Active*.
Initial incoming video	When initially joining a conference the received video may be muted or active. The **default** is *Active*.
Cameras crossed	Whether the cameras on the endpoint are crossed or not. The setting will be used to work out the order in which to display the screens of this endpoint on other endpoints in the conference. The **default** is *Not crossed*.
Bypass conference PIN entry	Whether to bypass the conference PIN entry screen. A number of older multiscreen endpoints do not allow the user to enter PINs and PIN entry has to be bypassed. We strongly recommend that you do not bypass PIN entry unless the endpoint does not support PIN entry. The **default** is *Do not bypass PIN entry*.

Field	Description
Legacy TIP endpoint	Whether TIP (Telepresence Interoperability Protocol) negotiation should be forced on this endpoint. We strongly recommend that you select *No*, unless the endpoint explicitly needs this configuration. If you select *Yes* for an endpoint that does not support TIP, the call will fail. If you select *Yes* for an endpoint that supports TIP, although the call will succeed, not all functionality may be available. The endpoints that require this setting to be *Yes* include: ■ CTS endpoints running versions 1.7.3 or earlier. ■ Polycom HDX/OTX systems. ■ CTS or TX endpoints that have their calls routed through a Unified CM running versions 8.0 or earlier. The **default** is *No*.
Codec layout order	(Only displayed when at least two codecs have been created for this endpoint) The order in which the codecs are arranged for this pre-configured endpoint. Drag the codecs into the correct order.

After creating a pre-configured endpoint, at least one codec has to be added to it.

If two or more codecs have been added you can configure the following settings:

- **Codec layout order**: the order in which the codecs are arranged for this pre-configured endpoint. In the **Configuration** section drag the codecs into the correct order.
- **Single screen audio**: the codec which receives audio from any single-screen endpoints in the conference. In the **Codecs** section select the appropriate codec.
- **Single screen content**: the codec which displays content from any single-screen endpoints in the conference. In the **Codecs** section select the appropriate codec.

Adding and editing pre-configured endpoint codecs

Each pre-configured endpoint must have at least one and at most four codecs configured.

Telepresence Interoperability Protocol (TIP) negotiated multiscreen endpoints, such as CTS and T3, only require the primary codec to be pre-configured.

To add a new codec to an existing pre-configured endpoint:

1. Go to the **Pre-configured endpoints** page (**Conference configuration > Pre-configured endpoints**).
2. Select a pre-configured endpoint to add a codec to.
3. Click **Create codec** in the **Codec** section.

When adding or editing a pre-configured endpoint codec, the configurable options are:

Field	Description
Name	A descriptive name of the pre-configured endpoint codec.
Description	A free-form description of the codec.

Field	Description
Pre-configured endpoint	The pre-configured endpoint to which this codec belongs. This is not configurable.
Protocol	The protocol the codec uses. The options are *H.323* or *SIP*. The protocol is only required for outgoing codecs. The **default** is *SIP*.
Address	The SIP or H.323 address of the codec. The SIP address is the endpoint's SIP URI, and the H.323 address can be one of the endpoint's E164 number(s) or H.323 ID(s). All codec addresses must be unique.
Optional address 1-5	Additional SIP or H.323 addresses for the codec. The codec may appear to be at a different address when registered to a cluster of call control devices. All possible addresses, from which calls for this codec could come in, must be added here. All codec addresses must be unique.
Direction	The direction of call signaling from the conference bridge's perspective. *Incoming*: The codec must call into the conference. *Outgoing*: The conference bridge will call the codec. At least one codec within a pre-configured endpoint should have a direction of *Incoming*, otherwise the endpoint cannot receive any calls.
Maximum quality	The video and audio quality setting that this codec will use. It will override the setting selected for the associated conference template. Depending on the selected setting the appropriate resources are allocated on the TelePresence Server. The quality settings can be changed on the **Quality settings** page. The initial list of quality settings includes: ■ Full HD (1080p 30fps / 720p 60fps video, multi-channel audio) ■ HD (720p 30fps video, stereo audio) ■ SD (wide 448p 30fps video, mono audio) The **default** is *HD (720p 30fps video, stereo audio)*.

Using Call Policy

About Call Policy

This feature is only applicable to Cisco VCS- based deployments.

When Call Policy is in use, the TelePresence Conductor will check with the Cisco TelePresence Video Communication Server (Cisco 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 a 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 Cisco VCS.

In a Cisco VCS-based deployment, there must not be any conflict between any **Incoming alias** or **Conference name** (used when Creating and editing conference aliases [p.78]), the Call Policy prefix [p.18], and Conference bridge dial plan prefixes [p.18], otherwise you may experience unpredictable behavior. For more information, see Considerations in a Cisco VCS-only deployment [p.18].

When to use Cisco VCS or TelePresence Conductor Call Policy

The TelePresence Conductor's Call Policy works in conjunction with the Cisco 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 Cisco VCS only, or on both the Cisco VCS and TelePresence Conductor depends on the desired result, as follows:

- **To prevent a user from creating or joining any conferences:** use Cisco 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 Cisco 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 Cisco 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 Cisco 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 with Cisco TelePresence Video Communication Server 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 Cisco 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 Cisco 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 Cisco VCS.

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

Call allowed

Alice dials **meet.alice**.

The Cisco 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 Cisco VCS.

The Cisco VCS checks its Call Policy to see whether Alice is allowed to dial **create.meet.alice**. She is, so the Cisco 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 Cisco 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 Cisco 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.

Configuring users

This section provides information on how to configure the root account, administrator accounts, administrator groups and LDAP accounts.

Configuring administrator accounts 99
Configuring remote account authentication using LDAP 101
Configuring administrator groups 104
Password security 106
Configuring the root account 107
Resetting forgotten passwords 108

Configuring administrator accounts

The **Administrator accounts** page (**Users > Administrator accounts**) lists all the local administrator accounts that have been configured on the TelePresence Conductor, and lets you add, edit and delete accounts. There is one pre-configured administrator account, which can have its username and password changed.

The account credentials for the administrator accounts 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 (Cisco TMS) to access the TelePresence Conductor.

The administrator accounts can only be used when the **Administrator authentication source** on the **LDAP configuration** page (**Users > LDAP configuration**) has been set to *Local* 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.

Adding or editing administrator account details

You can edit the details for the pre-configured administrator account and add additional local administrator accounts. These accounts can be used to access the TelePresence Conductor over the web and API interfaces.

The configurable options are:

Field	Description	Usage tips
Name	The username for the administrator account.	Some names such as "root" are reserved. Local administrator account user names are case sensitive.
Access level	The access level of the administrator account: *Read-write*: allows all configuration information to be viewed and changed. This provides the same rights as the default **admin** account. *Read-only*: allows status and configuration information to be viewed only and not changed. Some pages, such as the **Upgrade** page, are blocked to read-only accounts. Default: *Read-write*	The access permissions of the currently logged in user are shown in the system information bar at the bottom of each web page.
Password	The password that this administrator will use to log in to the TelePresence Conductor.	All passwords on the TelePresence Conductor are encrypted, so you only see placeholder characters here. When entering passwords, the bar next to the **Password** field changes color to indicate the complexity of the password. You can configure the complexity requirements for local administrator passwords on the Password security page (**Users > Password security**). You cannot set blank passwords.

Field	Description	Usage tips
Web access	Determines whether this account is allowed to log in to the system using the web interface. Default: *Yes*	
API access	Determines whether this account is allowed to access the system's status and configuration using the Application Programming Interface (API). Default: *Yes*	This controls access to the XML and REST APIs by systems such as Cisco TMS.
State	Indicates if the account is enabled or disabled. Access will be denied to disabled accounts.	

Configuring remote account authentication using LDAP

The **LDAP configuration** page (**Users > LDAP configuration**) is used to configure an LDAP connection to a remote directory service for administrator account authentication.

The configurable options are:

Field	Description	Usage tips
LDAP configuration: this section allows you to enable or disable the use of LDAP for remote account authentication.		
Administrator authentication source	Defines where administrator login credentials are authenticated. *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*.	*Both* allows you to continue to use locally-defined accounts. This is useful while troubleshooting any connection or authorization issues with the LDAP server. Note that you cannot log in using an administrator 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 FQDN (or server address, if a DNS **Domain name** has also been configured) of the LDAP server.	If using TLS, the server address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.
FQDN address resolution	Defines 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	The IP port to use on the LDAP server.	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*.	When TLS is enabled, the LDAP server's certificate must be signed by an authority within the TelePresence Conductor's trusted CA certificates file.
Authentication configuration: this section specifies the TelePresence Conductor's authentication credentials to use when binding to the LDAP server.		

Field	Description	Usage tips
Bind DN	The distinguished name (case insensitive) used by the TelePresence Conductor when binding to the LDAP server. It is important to specify the DN in the order cn=, then ou=, then dc=	Any special characters within a name must be escaped with a backslash as per the LDAP standard (*RFC 4514*). Do not escape the separator character between names. The bind account is usually a read-only account with no special privileges.
Bind password	The password (case sensitive) 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*.	Enable Simple Authentication and Security Layer if it is company policy to do so.
Bind username	Username of the account that the TelePresence Conductor will use to log in to the LDAP server (case sensitive). Only required if SASL is enabled.	Configure this to be the sAMAccountName; Security Access Manager Account Name (in AD this is the account's user logon name).
Directory configuration: this section specifies the base distinguished names to use when searching for account and group names.		
Base DN for accounts	The ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	The Base DN for accounts and groups must be at or below the dc level (include all dc= values and ou= values if necessary). LDAP authentication does not look into sub dc accounts, only lower ou= and cn= levels.
Base DN for groups	The ou= and dc= definition of the Distinguished Name where a search for groups should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	If no **Base DN for groups** is specified, then the Base DN for accounts will be used for both groups and accounts.

Connection status

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

State = Active

No error messages are displayed.

State = Failed

The following error messages may be displayed:

Error message	Reason / resolution
DNS unable to do reverse lookup	Reverse DNS lookup is required for SASL authentication.
DNS unable to resolve LDAP server address	Check that a valid DNS server is configured, and check the spelling of the LDAP server address.
Failed to connect to LDAP server. Check server address and port	Check that the LDAP server details are correct.
Failed to setup TLS connection. Check your CA certificate	CA certificate, private key and server certificate are required for TLS.
Failure connecting to server. Returned code<return code>	Other non-specific problem.
Invalid Base DN for accounts	Check **Base DN for accounts**; the current value does not describe a valid part of the LDAP directory.
Invalid server name or DNS failure	DNS resolution of the LDAP server name is failing.
Invalid bind credentials	Check **Bind DN** and **Bind password**, this error can also be displayed if SASL is set to *DIGEST-MD5* when it should be set to *None*.
Invalid bind DN	Check **Bind DN**; the current value does not describe a valid account in the LDAP director. This failed state may be wrongly reported if the **Bind DN** is 74 or more characters in length. To check whether there is a real failure or not, set up an administrator group on the TelePresence Conductor using a valid group name. If TelePresence Conductor reports “saved” then there is not a problem (the TelePresence Conductor checks that it can find the group specified). If it reports that the group cannot be found then either the **Bind DN** is wrong, the group is wrong or one of the other configuration items may be wrong.
There is no CA certificate installed	CA certificate, private key and server certificate are required for TLS.
Unable to get configuration	LDAP server information may be missing or incorrect.

Configuring administrator groups

The **Administrator groups** page (**Users > Administrator groups**) lists all the administrator groups that have been configured on the TelePresence Conductor, and lets you add, edit and delete groups.

Administrator groups only apply if remote account authentication is enabled.

When an administrator logs in to the TelePresence Conductor web interface, their credentials are authenticated against the remote directory service and they are assigned the access rights associated with the group to which the administrator belongs. If the administrator account belongs to more than one group, the highest level permission is assigned.

The configurable options are:

Field	Description	Usage tips
Name	The name of the administrator group. It cannot contain any of the following characters: / \ [ ] : ; | = , + * ? > < @ "	The group names defined in the TelePresence Conductor must match the group names that have been set up in the remote directory service to manage administrator access to this TelePresence Conductor.
Access level	The access level given to members of the administrator group: *Read-write*: allows all configuration information to be viewed and changed. This provides the same rights as the default **admin** account. *Read-only*: allows status and configuration information to be viewed only and not changed. Some pages, such as the **Upgrade** page, are blocked to read-only accounts. *None*: no access is allowed. Default: *Read-write*	If an administrator belongs to more than one group, it is assigned the highest level permission for each of the access settings across all of the groups to which it belongs (any groups in a disabled state are ignored). See Determining the access level for accounts that belong in multiple groups [p.104] below for more information.
Web access	Determines whether members of this group are allowed to log in to the system using the web interface. Default: *Yes*	
API access	Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API). Default: *Yes*	This controls access to the XML and REST APIs by systems such as Cisco TMS.
State	Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups.	If an administrator account belongs to more than one administrator group with a combination of both *Enabled* and *Disabled* states, their access will be *Enabled*.

Determining the access level for accounts that belong in multiple groups

If an administrator account belongs to more than one administrator group, the effective settings for **Access level**, **Web access** and **API access** will be the highest of each group to which the account belongs. Any groups in a disabled state are ignored.

For example, if the following groups were configured:

Group name	Access level	Web access	API access
Administrators	Read-write	-	-
Region A	Read-only	Yes	-
Region B	Read-only	-	Yes
Region C	Read-only	Yes	Yes

the following table shows examples of the access permissions that would be granted for accounts that belong in one or more of those groups:

Groups belonged to	Access permissions granted
Administrators and **Region A**	read-write access to the web interface but no API access
Administrators and **Region B**	read-write access to the API interface, but no web interface access
Administrators and **Region C**	read-write access to the web and API interfaces
Region A only	read-only access to the web interface and no API access

Password security

The **Password security** page (**Users > Password security**) controls whether or not local administrator account passwords must meet a minimum level of complexity before they are accepted.

If **Enforce strict passwords** is set to *On*, all subsequently configured local administrator account passwords must conform to the following rules for what constitutes a strict password.

Configurable rules

The following rules apply by default but can be customized.

The password must contain at least 15 ASCII characters made up of at least:

- 2 numeric values ['0'..'9']
- 2 uppercase letters ['A'..'Z']
- 2 lowercase letters ['a'..'z']
- 2 special characters [such as '@' or '$']

You can also specify:

- the minimum number of the 4 character classes (numeric , lower case, upper case, and special characters) that must be present; use this setting if you want to mandate the use of 2-3 different character classes without requiring all of them to be present
- the maximum number of times the same character can be repeated consecutively; by default there is no restriction

Additional non-configurable rules

The following strict password rules always apply and cannot be configured. Passwords must not:

- be based on a dictionary word
- contain too many consecutive characters such as "abc" or "123"
- contain too few different characters
- be palindromes

If **Enforce strict passwords** is set to *Off*, no checks are made on administrator passwords.

Note that:

- Regardless of this setting, it is not possible to set a blank password for any administrator account.
- This setting affects local administrator account passwords only. It does not affect any other passwords used on the TelePresence Conductor such as in the local authentication database, LDAP server, external registration credentials, user account passwords, or administrator account passwords stored on remote credential directories.
- All passwords and usernames are case sensitive.

Configuring the 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 Configuring administrator accounts [p.99] 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 [p.108] 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 administrator password if you still have access to the root account

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

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

Resetting an administrator password or your root password via a serial connection

If you have forgotten the password for either an 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. Reboot 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 the username of the administrator account) 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.

Viewing status

This section describes how to view status information on the TelePresence Conductor, accessible via the **Status** menu.

Getting a status overview 110
Alarms 111
Conference bridge status 113
Conferences status 114
Conference participants 115
Call status information 116
Event Log 117
Configuration Log 119

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**).
Hardware 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.	
Serial number	The serial number of the hardware or virtual machine 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, see About upgrading software components [p.134].
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 About conference bridges [p.45] for more information regarding conference bridges.
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 [p.180].

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 active alarms 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. See Alarm severity [p.112] 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.

For each conference bridge the configuration status, the operational status, the conferences it is hosting and the resource usage is displayed.

When using a TelePresence Conductor without a release key, it is only possible to enable one conference bridge across all conference bridge pools. All other conference bridges have a **State** of *Busied out*. The conference bridge that is enabled cannot be clustered. If the only enabled conference bridge is clustered, its **Status** is *Unusable* and the TelePresence Conductor is unable to communicate with any conference bridges.

The resource usage on a TelePresence MCU is measured in number of ports. The resource usage on a TelePresence Server is measured in number of screen licenses and calls.

The utilization is determined by the largest value out of the allocated resources and the used resources for a particular conference bridge. The utilization bar is shown in green when the conference bridge utilization is below the threshold at which a conference bridge resource alarm should be raised; which can be configured on the **Global conference bridge settings** page (**Conference configuration > Conference bridges > Global conference bridge settings**). The utilization bar is shown in yellow when the conference bridge is approaching the threshold and in red when it has exceeded the threshold.

Allocated resources are those that have been requested on the TelePresence Conductor when the conference is first initiated. Used resources are those that the conference bridge actually uses when the conference is hosted on the conference bridge. Resource optimization can reduce the number of used resources on a TelePresence Server.

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.

A conference can have one of the following states:

- Starting
- Running
- Stopping

For each conference the number of participant resources that are reserved, requested or used are displayed. The information is displayed in summary, as well as for each conference bridge hosting the conference.

This release of the TelePresence Conductor does not support cascading of TelePresence Servers. Therefore the Cascade resources are always 0 for TelePresence Server and only the information for one conference bridge is displayed.

Chairperson resources can be reserved on conference templates for Lecture-type conferences. Participant resources, which apply to Meeting-type conferences and guest resources, which apply to Lecture-type conferences cannot be reserved.

Auto-dialed participant resources can be requested by creating an auto-dialed participant with a particular role type and associating it with a conference template.

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:

Participant	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	(Available when **Conference type** is *Lecture*) *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. Click on the address to go to the web interface for this conference bridge.
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.

Call status information

The **Status > Calls** pages provide information about the current and historic calls passing through the TelePresence Conductor. These pages list all calls from Unified CM for which TelePresence Conductor receives signaling, i.e. calls that Unified CM sends directly to TelePresence Conductor, without going through a SIP trunk between Unified CM and Cisco VCS, and calls from a Cisco VCS that do not use the Cisco VCS's external policy server interface.

Call status

Call status information can be displayed for both current and completed calls:

- **Current calls**: the **Call status** page (**Status > Calls > Calls**) lists all the calls currently passing through the TelePresence Conductor.
- **Completed calls**: the **Call history** page (**Status > Calls > Call history**) lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the TelePresence Conductor was last restarted.

If the TelePresence Conductor is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

Call summary information

The following summary information is displayed initially:

Field	Description
Start time	The date and time when TelePresence Conductor took the call.
End time	The date and time when the call ended on TelePresence Conductor (completed calls only).
Duration	The length of time of the call.
Source	The alias of the endpoint that placed the call.
Destination	The alias dialed from the endpoint. This will be different from the alias to which the call was placed, which will have been transformed.
Status	The reason the call ended (completed calls only). A call has a status of *Disconnected* when an administrator has terminated the call using the **Disconnect** button. A call has a status of *BYE* when either the caller or callee has terminated the call normally.
Peer	Identifies the cluster peer through which the call is being made.
Actions	Click **View** to see further information about the call.

Call detail information

After selecting a call from the primary list (as described above) you are shown further details of that call.

Disconnecting calls

Click **Disconnect** to disconnect the selected calls. Note that if your TelePresence Conductor is part of a cluster you have to be logged into the peer through which the call is passing to be able to disconnect the call.

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 > Logs > Event Log > All events**) lets you view and filter the Event Log.

The other sub-menus under the **Status > Log > 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

Configuration Log

The **Configuration Log** page (**Status > Logs > Configuration Log**) provides a list of all changes to the TelePresence Conductor configuration.

The Configuration Log holds a maximum of 30MB of data; when this size is reached, the oldest entries are overwritten. The entire Configuration Log can be displayed through the web interface.

Filtering the Configuration Log

The **Filter** section lets you filter the Configuration Log. 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.

Use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete Configuration Log listing, click **Reset**.

Results section

The **Results** section shows all the web-based events, with the most recent being shown first.

Most 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 **Event=** filters the list to show all the events of that particular type. Likewise, clicking on a particular **user** shows just those events relating to that particular administrator account.

Configuration Log events

Changes to the TelePresence Conductor configuration made by administrators using the web interface have an **Event** field of *System Configuration Changed*.

The **Detail** field of each of these events shows:

- the configuration item that was affected
- what it was changed from and to
- the name of the administrator user who made the change, and their IP address
- the date and time that the change was made

Clustering

This section provides information on how to configure a TelePresence Conductor to be part of a cluster of up to three TelePresence Conductor systems.

About clusters 121
Peer-specific configuration 122
Creating a new cluster 124
Changing a peer's IP address 127
Removing a peer from an existing cluster 128
Disbanding a cluster 130
Upgrading a cluster 131
Cluster backup and restore 132

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).

Note: clustering of the TelePresence Conductor is not supported when the TelePresence Conductor is running without a release key.

To avoid confusion, we recommend that you make all configuration changes on one peer. The only exception to this is any Peer-specific configuration [p.122].

For more information, see the relevant deployment guide:

- *Cisco TelePresence Conductor Clustering with Cisco Unified CM Deployment Guide*,
- *Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS Deployment Guide*, or
- *Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS (B2BUA) 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 [p.127] 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.

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 (including the peer's own IP address) 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.

Any additional IPv4 addresses added for use with Unified CM must be different for each peer in the cluster.

Note: the only IP settings that can be changed when the system is part of a cluster are the additional IPv4 addresses. Primary LAN 1 IP address settings cannot be changed.

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 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 and Configuration 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 Logging configuration [p.137] 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.

Unified CM locations

All ad hoc or rendezvous IP addresses assigned to Unified CM locations must be different for each peer in the cluster.

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 inline **Status** shows the current status of each peer.

Prerequisites

Before you create the cluster:

- Ensure that the TelePresence Conductor is running with a valid release key.
  Clustering is not supported on TelePresence Conductors that are running without a release key.
- 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.
- If peers are deployed on different LANs, there must be sufficient connectivity between the networks to ensure a low degree of latency between the peers - a maximum delay of 15ms one way, 30ms round-trip.
- Note that 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.
   Subsequently configuration on any peer will be shared with all other peers, because every peer is treated equally.
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.
   The IP address must be the primary LAN 1 IP address. Do not use an additional IP address that may have been configured on the peer.
5. **Save** this configuration.
6. Restart this peer (**Maintenance > Restart options**, then click **Restart**).

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 [p.128] 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 options**, then click **Restart**).
7. Log in to the new peer.
   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 [p.125].

Updating configuration on the call control devices

In a Cisco VCS-based deployment

When you have created a cluster of TelePresence Conductors in a Cisco VCS-based deployment, you must ensure that the relevant policy service on the Cisco VCS is updated with details of all the peers in the cluster.

In a Unified CM-based deployment

When you have created a cluster of TelePresence Conductors in a Unified CM-based deployment, you must ensure that:

- (for all rendezvous conferences and ad hoc conferences with outbound calls) the SIP trunk settings on the Unified CM are updated with details of all the peers in the cluster.
- (for all ad hoc conferences) the media resource group and conference bridge settings are updated on the Unified CM.

Monitoring the status of the cluster

The inline status areas 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. See Removing a peer from an existing cluster [p.128] 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. See Adding new peers to the cluster [p.125] 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, see Disbanding a cluster [p.130].

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 [p.129].

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 [p.128] and Adding new peers to the cluster [p.125].

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 options**, then click **Restart**).
6. Delete all entries from the conference bridge pool.
7. If using a Cisco VCS, update the policy service on the Cisco VCS so that it does not include the removed peer.

The peer will no longer consider itself part of the cluster. The peer will become unusable and no calls will go through it. You must now follow the instructions in Removing the peer from the cluster [p.129].

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, see Removing a peer from an existing cluster [p.128].

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 options**, then click **Restart**).
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:

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

For detailed instructions on upgrading a cluster, see the relevant deployment guide:

- *Cisco TelePresence Conductor Clustering with Cisco Unified CM Deployment Guide*,
- *Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS Deployment Guide*, or
- *Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS (B2BUA) Deployment Guide*.

Note: you should backup the system configuration of each peer before upgrading. For more information, see Cluster backup and restore [p.132].

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 [p.122]) 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, see Backing up and restoring data [p.147].

Maintenance

This section provides information on how to perform the TelePresence Conductor maintenance tasks, accessible via the **Maintenance** menu.

About upgrading software components 134
Logging configuration 137
Add option and release keys 138
About the Tools menu 139
Trusted CA Certificate 144
Managing the TelePresence Conductor's server certificate 145
Backing up and restoring data 147
Diagnostic logging 149
Creating a system snapshot 151
Incident reporting 152
Viewing or deleting feedback receivers 155
Restarting, rebooting and shutting down 156
Developer resources 158

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 [p.134] prior to upgrading your software.

For information about upgrading peers in a cluster of TelePresence Conductors, see Upgrading a cluster [p.131].

Before you upgrade

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 either:
- *Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide*, or
- *Cisco TelePresence Conductor Clustering with Cisco Video Communication Server Deployment Guide*

Prerequisites

The upgrade requires you to have:

- a valid **Release key**, if you are upgrading the major release of the TelePresence Conductor (for example from XC1.0 to XC2.1).
  A release key is not required for:
  - dot releases (for example XC2.0 to XC2.1), and
  - systems that are running without a release key before the upgrade and should continue to run without a release key (with limited capacity) after the upgrade.
    Note: it is not possible to upgrade the major release without a release key if the system currently has a valid release key installed.
- 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.

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 [p.134] 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.
  Note: if a call goes through the TelePresence Conductor's back-to-back user agent, a reboot will cause all active calls to be terminated. If the TelePresence Conductor is using the Cisco VCS's external policy server interface, a reboot will not affect existing conferences; these will be left running. 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 re-join existing conferences.
- For additional information about upgrading peers in a cluster, see Upgrading a cluster [p.131].

To upgrade 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 starting the upload process 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 server**s 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 [p.117].

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.

- You can configure the TelePresence Conductor to copy event log messages to up to 4 remote syslog servers.
- The syslog server must support the BSD (as defined in *RFC 3164*) or IETF (as defined in *RFC 5424*) syslog protocols.

Configuring a remote syslog server

To enable remote logging, configure the TelePresence Conductor with the IP addresses or Fully Qualified Domain Names (FQDNs) of the **Remote syslog servers** to which the Event Log will be written.

For each server you must also specify the syslog protocol **Mode** to use when sending messages to that server, either *Legacy BSD format*, *IETF syslog format* or *IETF using TLS connection*. Alternatively, choose *Custom* to configure individually the **Transport**, **Port** and **Format** to use.

If a TLS connection is used you must ensure that a suitable CA certificate file and certificate revocation lists (CRLs) have been configured on the TelePresence Conductor. Note that CRL checking is disabled by default; to enable CRL checking you must select the *Custom* mode, set **CRL check** to *On* and ensure that relevant certificate revocation lists (CRLs) are loaded. See Trusted CA Certificate [p.144] for more information.

Note that:

- The remote server cannot be another TelePresence Conductor.
- A TelePresence Conductor cannot 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 is configured, the same information is sent to each server.
- 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 software components of the TelePresence Conductor.

Add option and release keys

The **Option keys** page (**Maintenance > Option keys**) lists all the existing options currently installed on the TelePresence Conductor, and allows you to add new options. It also displays the currently installed release key for this software version and allows you to enter a new release key.

Options are used to add additional features to the TelePresence Conductor. Option keys can either be valid for a fixed time period or have an unlimited duration. It is not possible to purchase additional option keys for this version of the TelePresence Conductor.

The **System information** section displays the **Hardware serial number** and summarizes the existing features installed on the TelePresence Conductor. The options that you may see here include:

- Bridge enablement limit
- Call session limit
- Clustering

Adding option keys using the web interface

To add an option key:

1. In the **Add option key** field, enter the key that has been provided to you for the option you want to add.
2. Click **Add option**.

Some option keys require that the TelePresence Conductor is restarted before the option key takes effect. In such cases an alarm is raised, which remains in place as a reminder until the system has been restarted.

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 details of the route taken by a network packet sent from the TelePresence Conductor to a particular destination host system.
- Tracepath allows you to discover the path taken by a network packet sent from the TelePresence Conductor to a particular destination host system.
- DNS lookup [p.142] 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 [p.162].

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.

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 try 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 system to which you want to trace the path.
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.

Tracepath

The **Tracepath** tool (**Maintenance > Tools > Network utilities > Tracepath**) 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.

To use this tool:

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

A new section will appear with a banner stating the results of the trace, and showing the details of each router along the path, the time taken for each router to respond to the request, and the maximum transmission units (MTU).

The route taken between the TelePresence Conductor and a particular host may vary for each tracepath 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 query DNS for a supplied hostname and display the results of the query if the lookup was successful.

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. 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**.

Managing the TelePresence Conductor's server certificate

The **Server certificate** page (**Maintenance > Security certificates > Server certificate**) is used to manage 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. You can:

- view details about the currently loaded certificate
- generate a certificate signing request
- upload a new server certificate

Viewing the currently uploaded certificate

The **Server certificate data** section shows information about the server certificate currently loaded on the TelePresence Conductor.

- To view the currently uploaded server certificate file, click **Show server certificate**.
- To replace the currently uploaded server certificate with the TelePresence Conductor's default certificate, click **Reset to default server certificate**.

Note: do not allow your server certificate to expire as this may cause other external systems to reject your certificate and prevent the TelePresence Conductor from being able to connect to those systems.

Generating a certificate signing request (CSR)

The TelePresence Conductor can generate server certificate signing requests. This removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

1. Go to **Maintenance > Security certificates > Server certificate**.
2. Click **Generate CSR** to go to the **Generate CSR** page.
3. Enter the required properties for the certificate.
   - See Server certificates and clustered systems [p.146] if your TelePresence Conductor is part of a cluster.
   - The certificate request includes automatically the public key that will be used in the certificate, and the client and server authentication Enhanced Key Usage (EKU) extension.
4. Click **Generate CSR**. The system will produce a signing request and an associated private key. Note that the private key is stored securely on the TelePresence Conductor and cannot be viewed or downloaded. You must never disclose your private key, not even to the certificate authority.
5. You are returned to the **Server certificate** page. From here you can:
   - **Download** the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).
   - **View** the current request.

Note that only one signing request can be in progress at any one time. This is because the TelePresence Conductor has to keep track of the private key file associated with the current request. To discard the current request and start a new request, click **Discard CSR**.

When the signed server certificate is received back from the certificate authority it must be uploaded to the TelePresence Conductor as described below.

Uploading a new server certificate

The **Upload new certificate** section is used to replace the TelePresence Conductor's current server certificate with a new certificate.

To upload a server certificate:

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

Server certificates and clustered systems

When a CSR is generated, a single request and private key combination is generated for that peer only.

If you have a cluster of TelePresence Conductors, you must generate a separate signing request on each peer. Those requests must then be sent to the certificate authority and the returned server certificates uploaded to each relevant peer.

You must ensure that the correct server certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.

Backing up and restoring data

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

Backing up and restoring overview [p.147] gives information about when to create a backup, the contents of the backup file, and limitations you should be aware of.

Creating a backup [p.148] describes how to backup TelePresence Conductor data.

Restoring a previous backup [p.148] describes how to restore TelePresence Conductor data.

For extra information about backing up and restoring peers in a cluster, see Cluster backup and restore [p.132].

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

Note that log files 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, see Cluster backup and restore [p.132].

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.

Diagnostic logging

The **Diagnostic logging** tool (**Maintenance > Diagnostics > 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.

In order to collect comprehensive information for debugging purposes, it is recommended to extract the diagnostic log for each peer in a cluster.

Creating a system snapshot

The **System snapshot** page (**Maintenance > Diagnostics > 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, and Configuration 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.

If your TelePresence Conductor is part of a cluster, it is recommended to create a system snapshot file on each individual cluster peer. Not all information is replicated across the cluster peers.

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.

Incident reporting caution: 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 are always saved locally, and can be viewed via the Incident view page.

Sending incident reports automatically

Read the privacy-protected personal data caution 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 > Diagnostics > 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/`.

4. Optional. Specify a **Contact email address** that can be used by Cisco customer support to follow up any error reports.
5. Optional. Specify a **Proxy server** to use for the connection to the incident reporting server.
6. Ensure that **Create core dumps** is *On*; this is the recommended setting as it provides useful diagnostic information.

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

Read the privacy-protected personal data caution 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 > Diagnostics > 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 > Diagnostics > 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 > Diagnostics > 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 > Diagnostics > 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 a 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, read the caution regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

Viewing or deleting feedback receivers

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

Whenever Cisco TMS or PCM register for feedback from TelePresence Conductor an entry for the Cisco 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, rebooting and shutting down

The **Restart options** page (**Maintenance > Restart options**) allows you to restart, reboot or shut down the TelePresence Conductor without having physical access to the hardware.

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

Restarting

The restart function shuts down and restarts the TelePresence Conductor application software, but not the operating system or hardware. A restart takes approximately 2 minutes.

A restart is typically required in order for some configuration changes to take effect, or when the system is being added to, or removed from, a cluster. In these cases a system alarm is raised and will remain in place until the system is restarted.

If the TelePresence Conductor is part of a cluster and other peers in the cluster also require a restart, we recommend that you wait until each peer has restarted before restarting the next peer.

Rebooting

The reboot function shuts down and restarts the TelePresence Conductor application software, operating system and hardware. A reboot takes approximately 5 minutes.

Reboots are normally only required after software upgrades and are performed as part of the upgrade process. A reboot may also be required when you are trying to resolve unexpected system errors.

Shutting down

A shutdown is typically required if you want to unplug your unit, prior to maintenance or relocation for example. 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.

Effect on conferences

If a call goes through the TelePresence Conductor's back-to-back user agent, any of these restart options will cause all active calls to be terminated.

If the TelePresence Conductor is using the Cisco VCS's external policy server interface,none of the restart options will affect existing conferences; these will be left running. If the TelePresence Conductor is part of a cluster, users can still create, join or re-join conferences while an individual peer is restarting. If it is not part of a cluster, users will not be able to create new conferences, or join or re-join existing conferences.

Restarting, rebooting or shutting down using the web interface

To restart the TelePresence Conductor using the web interface:

1. Go to **Maintenance > Restart options**.
2. Click **Restart**, **Reboot** or **Shutdown** as appropriate and confirm the action.
   Sometimes only one of these options, such as **Restart** for example, may be available. This typically occurs when you access the **Restart options** page after following a link in an alarm or a banner message.

- Restart/reboot: the **Restarting**/**Rebooting** page appears, with an orange bar indicating progress. After the system has successfully restarted or rebooted, you are automatically taken to the **Login** page.
- Shutdown: 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.

Software version history 160
Regular expression reference 162
Conference layouts 170
Port reference 173
Event Log reference 174
Restoring default configuration 176
Identifying calls across your network 177
Password encryption 178
Flash status word reference table 179
Alarm categories 180
Bibliography 181
Glossary 182
Legal notices 186
Accessibility notice 187

Software version history

This section summarizes feature updates that have occurred in earlier software releases.

XC2.0

Cisco TelePresence Server support

A new conference bridge type of Cisco TelePresence Server is supported in this release of the TelePresence Conductor. Conference bridge pools can now be made up of either TelePresence Servers or TelePresence MCUs.

Cisco Unified Communications Manager support

The TelePresence Conductor now supports direct connection to Cisco Unified Communications Manager for ad hoc and rendezvous calls. Endpoints can be registered with either Unified CM or Cisco VCS and call into the same conference.

Addition of multiple IP addresses

Multiple IP addresses can be added on TelePresence Conductor. A different IP address is needed on the TelePresence Conductor for each ad hoc Unified CM location and each rendezvous Unified CM location. This allows the TelePresence Conductor to mimic Unified CM's expectation that it is connecting to separate conference bridges in each location, for ad hoc and rendezvous calls.

Known and unknown multiscreen endpoint support for TelePresence Server conferences

The TelePresence Conductor supports endpoints with more than one screen in conferences hosted on TelePresence Servers.

Cisco TelePresence System (CTS) series endpoints, including Cisco TelePresence System T3, can be pre-configured, in which case they will be allocated the resources defined for the endpoint, or supported without pre-configuration, in which case they will be allocated the resources defined for the conference template.

Other customized multiscreen endpoints have to be pre-configured if sufficient resources are to be allocated on the TelePresence Servers used in the relevant conferences.

Support for third-party and customized multiscreen TelePresence systems (i.e. those other than CTS3xxx, TX9000 or T3) require the optional third-party interop key on the TelePresence Server.

Resource optimization

Resource optimization allows resources that are initially over-allocated on a TelePresence Server to be recovered and re-allocated for other participants, allowing more participants to be handled by a single TelePresence Server.

XML-RPC API support to communicate between Cisco TMS and TelePresence Server 3.0

The TelePresence Conductor API now has support added to translate information being sent between Cisco TelePresence Management Suite and TelePresence Server version 3.0 running in 'Remotely managed' mode. See *Cisco TelePresence Management Suite Release Notes* for information on when this support has been added to the Cisco TMS.

Improvements to logging

Filtered event logs can now be downloaded from the UI.

It is possible to specify the remote syslog server mode as one of the following:

- Legacy BSD format
- IETF syslog format
- IETF syslog using TLS connection
- Custom

The Configuration Log page provides a list of all changes to the TelePresence Conductor configuration, providing users with an audit trail of the TelePresence Conductor configuration.

System Administration session timeout and limits

It is now possible to set a session time out, as well as limits for concurrent sessions and concurrent logins per administrator account for web, SSH and serial sessions.

Certificate signing request (CSR)

The TelePresence Conductor can now generate server certificate signing requests, which removes the need to use an external mechanism to generate and obtain certificate requests.

Firewall rules

Firewall rules can now be added to the TelePresence Conductor, which provide the ability to configure IP table rules to control access to the TelePresence Conductor at the IP level.

Addition of multiple administrator accounts

It is now possible to add multiple administrator accounts with pre-determined access level settings.

Other changes and improvements

Improvements have been made to the TelePresence Conductor web interface.

Regular expression reference

This section provides the following information about regular expressions:

- About regular expressions [p.162] provides a table of common regular expressions.
- Regular expression examples - conference aliases [p.163] 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 [p.78] and when Creating and editing auto-dialed participants [p.80].

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 Python 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 [p.163]
- 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 [p.166].

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 must resolve to the same string. 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 [p.163], 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 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 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.** 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.	
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 three tables displaying the layouts that can be selected for TelePresence MCUs and TelePresence Servers.

TelePresence MCU layouts

Layout families

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

index	Example layouts
1	
2	
3	
4	
5	

Specific layouts

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

index	Layout	index	Layout	index	Layout	index	Layout
1		16		31		46	
2		17		32		47	
3		18		33		48	
4		19		34		49	

index	Layout	index	Layout	index	Layout	index	Layout
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			

TelePresence Server layouts

There are four different layouts on the TelePresence Server, all of which are supported on single-screen endpoints and two of which are supported on multiscreen endpoints.

Layout	Name	Description
	Single	**On a single-screen endpoint**: the active speaker is shown in one full-screen pane. **On a multiscreen endpoint**: all screens of the endpoint with the active speaker are shown full-screen.

Layout	Name	Description
	ActivePresence	**On a single-screen endpoint**: the active speaker is shown in a large pane with additional participants appearing in up to nine PIPs (picture-in-pictures) overlaid at the bottom of the screen. **On a multiscreen endpoint**: all screens of the endpoint with the active speaker are shown full-screen, additional participants appear in up to nine PIPs (picture-in-pictures) overlaid at the bottom of the screen.
	Prominent	**On a single-screen endpoint**: the active speaker is shown in a large pane with additional participants appearing in up to four smaller panes at the bottom of the screen.
	Equal	**On a single-screen endpoint**: conference participants are shown in a grid pattern of equal sized panes, up to 4x4.

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.

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
SSH	Used for encrypted command line administration.	22 TCP	inbound
NTP	Used for updating the system time (and important for H.235 security).	123 UDP	outbound
SNMP	Used for network management.	161 UDP	inbound
HTTP	Used for unencrypted web administration. Redirects HTTP requests to HTTPS.	80 TCP	inbound
HTTPS	Used for encrypted web administration.	443 TCP	inbound and outbound
Clustering	Used for communication between cluster peers	4369-4380 TCP	inbound and outbound
Clustering	Used to recover from intra-cluster communication failure	4371 UDP	inbound
Clustering	Used for IPSec secure communication between cluster peers.	500 UDP	inbound
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 [p.174] 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**. Following the **Event** is a list of parameters with corresponding values. The last element is always **UTCTime**. The table below describes these elements.

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.

Name	Description
Detail	Descriptive detail of the event.
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

You can 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 [p.117] and Configuration Log [p.119], 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 (Cisco VCSs). When a Cisco VCS receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the Cisco 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 Cisco VCS or a TelePresence Conductor. A single call passing between two or more Cisco 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 Cisco VCS or TelePresence Conductor, or a Cisco 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 administrator accounts
- 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	1024	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 the TelePresence Conductor can be found at www.cisco.com.

Title	Reference	Link
Cisco TelePresence Conductor Clustering with Cisco Unified CM Deployment Guide	D15000	www.cisco.com
Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS Deployment Guide	D14828	www.cisco.com
Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS (B2BUA) Deployment Guide	D15034	www.cisco.com
Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide	D14998	www.cisco.com
Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server Deployment Guide	D14827	www.cisco.com
Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server (B2BUA) Deployment Guide	D15014	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 Server API 3.0 Reference Guide	D15003	www.cisco.com
Cisco TelePresence Server Online Help	D14510	www.cisco.com
Cisco TelePresence Video Communication Server Administrator Guide	D14049	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 3164: The BSD syslog Protocol		http://tools.ietf.org/html/rfc3164
RFC 3261: SIP: Session Initiation Protocol		http://tools.ietf.org/html/rfc3261
What warnings do I get on a Cisco TelePresence MCU that my conference is finishing? (knowledge base article)		www.cisco.com

Glossary

Term	Definition
1080p	A high definition (HD) display resolution, often referred to as Full HD. The 1080 refers to a vertical display resolution of 1080 pixels, with a horizontal display resolution of 1,920 pixels. The p refers to progressive scan; any figure after the p refers to the frame rate.
720p	A high definition (HD) display resolution. The 720 refers to a vertical display resolution of 720 pixels, with a horizontal display resolution of 1,280 pixels. The p indicates progressive scan; any figure after the p refers to the frame rate.
480p	A standard definition (SD) video display resolution. It is more likely to be used in video conferencing solutions than in telepresence. The 480 refers to a vertical display resolution of 480 pixels, usually with a horizontal display resolution of 640 pixels. The p refers to progressive scan; any figure after the p refers to the frame rate.
ActivePresence	A Cisco TelePresence screen layout that maintains the face-to-face immersive experience whilst displaying passive participants in small video panes.
Ad hoc conference	A non-scheduled, spontaneous meeting where a user brings two or more people together in a conference that has not been pre-planned.
Alias	The name an endpoint uses when registering with a call control device. Other endpoints can then use this name to call it. An endpoint may register with more than one alias.
AOR Address of Record	A SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.
Auto-dialed participant	A participant whose address is automatically dialed by the conference bridge when the conference starts. 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 [p.80].
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. This is applicable to a Cisco VCS-based deployment. For more information, see Using Call Policy [p.95].
Call Tag	A UUID common to all forks of a call across a network of TelePresence Conductors and Cisco VCSs. For more information, see Call Tags [p.177].
Cascade	The part of a conference that is being hosted on a secondary conference bridge. Conferences are cascaded to a secondary conference bridge when the primary conference bridge does not have enough ports available for all the participants. This feature is currently only supported on TelePresence MCUs. For more information, see Reserving cascade ports [p.73].
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 [p.87].

Term	Definition
Cluster	A collection of two or three TelePresence Conductor units that have been configured to work together in order to provide redundancy.
Codec	Shortened form of coder/decoder. Codecs are software or hardware which compress (for transmission) and decompress (when received) digital video and analog audio signals so that they occupy less bandwidth during transmission. Multiscreen endpoints may have more than one codec. All codecs have to be pre-configured for the TelePresence Conductor to support the endpoint. For more information, see Creating and editing pre-configured endpoints [p.91].
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 [p.78].
Conference bridge	A network device that allows multiple endpoints to participate in a video conference, for example an MCU (Multipoint Control Unit).
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 About conference bridges [p.45] and Selecting the preferred conference bridges for a conference [p.60].
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 [p.18].
External manager	The remote system that is used to manage endpoints and network infrastructure. The Cisco TelePresence Management Suite (Cisco TMS) is an example of an external manager.

Term	Definition
Guest	A participant who does not have chairperson privileges on the conference bridge. For more information, see About chairperson and guest roles [p.87].
H.323	A standard that defines the protocols used for packet-based multimedia communications systems.
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.
Multiway (Cisco TelePresence Multiway)	A feature that allows three or more endpoints to join a point-to-point meeting. Multiway does this using MCU resources.
Participant	A person or device who has joined a conference. Each 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 reserved resources.
Peer	A TelePresence Conductor unit that has been configured to belong to a cluster.
PiP	Picture in Picture. A smaller window within the screen of an endpoint.
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. For more information, see About regular expressions [p.162].
Rendezvous conference	A non-scheduled conference for which the host knows the conference alias beforehand, and must share the alias with all participants. Participants can join at any time, and there is no scheduled end time.
Reserved participant	A participant for whom resources have been specifically reserved. For this release of the TelePresence Conductor, you can only reserve resources for chairpersons. For more information, see Reserving chairperson participants [p.73].
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 [p.60].
SIP Session Initiation Protocol	IETF protocol for controlling multimedia communication. Defined by *RFC 3261*.

Term	Definition
Source alias	The alias present in the “source” field of a message.
TIP	Telepresence Interoperability Protocol. A Cisco protocol that enables interoperability between telepresence endpoints from different vendors.
Unified CM location	A Unified CM location is required in a Unified CM-based deployment. It is used to mimic the Unified CM's expectation that is it connecting to separate conference bridges in different physical locations.

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 section.

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2013 Cisco Systems, Inc. All rights reserved.