Cisco TelePresence TelePresence Server 8710 and 7010 Version 3.0

Remotely Managed Mode Printable Online Help

D15006

December 2012

Contents

Introduction

This document contains the text of the online help for the Cisco TelePresence Server version 3.0 web user interface. It is provided so that the help text can be viewed or printed as a single document.

This document accompanies version 3.0 of the TelePresence Server software when operating in remotely managed mode. This software is used on the following Cisco TelePresence hardware:

- Cisco TelePresence Server 7010
- Cisco TelePresence Server MSE 8710 blade

The contents of this document are organized in a similar way to the product's user interface, and replicate the contents of its online help system.

There is a chapter for each of the main interface pages and each chapter's title page contains a list of topics in the chapter.

Further information

See the online help for details of software licenses relating to this product.

Logging into the web interface

Why do I need to log in to the web interface?

The TelePresence Server restricts user access by holding a set of pre-configured accounts and denying access to anyone who does not have an account. Each account has a username and password that enables the account owner to gain access to their associated privileges.

There are two types of user account, each with different privileges:

- Administrators—may access all functionality
- API access—can only access the API, not the web interface

Tasks

Logging in to the web interface:

1. Enter the host name or IP address of the TelePresence Server into the address bar of a web browser. The log in page displays.
2. Enter your assigned **Username** and **Password**.
3. Click **OK**.

Failing to log into the web interface

Why am I seeing the **Access denied** page?

You have not been able to log in for one of the following reasons:

- **Invalid username/password**: you have typed the incorrect username and/or password.
  If Advanced account security mode is enabled and you incorrectly enter an account's credentials three times, then the TelePresence Server disables the account. The account is disabled for 30 minutes if it is an administrator account. The account is disabled indefinitely if it is another type of account. Administrators can re-enable accounts on the **User** page.
- **No free sessions**: the maximum number of sessions allowed simultaneously on the TelePresence Server has been reached.
- **Your IP address does not match that of the browser cookie you supplied**: try deleting your cookies and log in again
- **You do not have access rights to view this page**: you do not have the access rights necessary to view the page that you attempted to see
- **Page expired**: the **Change password** page can expire if the TelePresence Server detects that the user who requested to change password, may not actually be the user submitting the change password request. (This may happen if you use a new browser tab to submit the request.)

System status

Displaying system status

The **Status** page displays an overview of the TelePresence Server's status. To access this information, go to **Status**.

Refer to the table below for details of the information displayed.

System status

Field	Field Description	Usage tips
Model	The specific TelePresence Server model.	
Serial number	The unique serial number of the TelePresence Server.	You will need to provide this information when speaking to customer support.
Software version	The installed software version.	
Build	The build version of installed software.	
Uptime	The time since the last restart of the TelePresence Server.	
Host name	The host name assigned to the TelePresence Server.	
IP address	The IP address assigned to the TelePresence Server.	
IPv6 address	The IPv6 address of this TelePresence Server.	
H.323 gatekeeper status	Whether the TelePresence Server is registered to an H.323 gatekeeper, and whether the registration has been made to the primary or an alternate gatekeeper.	This field is only displayed on the master blade in a TelePresence Server cluster.
SIP registrar status	Whether the TelePresence Server is registered to a SIP registrar.	This field is only displayed on the master blade in a TelePresence Server cluster.
Enhanced font	Indicates whether the TelePresence Server is using a TrueType font file to render text.	*In use* or *Not in use*, depending on whether you have uploaded the font file. If it is *Not in use*, the TelePresence Server falls back on the default text rendering method.
Operation Mode	Indicates whether the TelePresence Server is operating in locally managed or remotely managed mode.	

Activated features

Field	Field description	Usage tips
TelePresence Server activation	Whether or not the unit is enabled.	The TelePresence Server will not operate without activation. This feature and key are installed before shipping.

Field	Field description	Usage tips
Encryption	Whether or not encryption is enabled.	The encryption feature key allows encrypted conferences and HTTPS web management on this blade. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server.
Third party interop	This feature allows the TelePresence Server to interoperate with third party multi-screen endpoints. (Note that only some third party multi-screen endpoints require this key.) It also activates the grouped endpoints features.	This field is only displayed if you have the appropriate key installed. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server Calls to general third party endpoints will work without this key. It is required to support multi-screen third party endpoints, such as the Polycom RPX and endpoint groups.
Cluster support	This feature allows blades configured on the same Cisco TelePresence MSE 8000 chassis to be linked together to behave as a single unit.	Up to four blades can form a cluster. See Understanding clustering. If you want to cluster a blade, the blade must have the cluster support feature key installed. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server
Screen licenses	The number of screen licenses in use across all active conferences. The total number of screen licenses may be less than the total number that the TelePresence Server can support.	You need to install a screen license key to enable screen licenses.

Conference status

Field	Field description	Usage tips
Active conferences	The number of active conferences on this TelePresence Server.	A conference is active if it has participants.
Active participants	The number of participants (of all types) that are currently in conferences on this TelePresence Server.	
Previous participants	The number of participants who were previously participating in a conference (since the last time the TelePresence Server restarted).	
Video ports	The number of video ports in use on this TelePresence Server.	The numbers are those supported by the number of screen licenses available on the TelePresence Server and dependent upon whether the TelePresence Server is configured to run in HD or Full HD mode.
Audio ports	The number of audio-only ports in use on this TelePresence Server.	
Content ports	The number of content channel ports in use on this TelePresence Server.	

System log

Field	Field description	Usage tips
	The system log displays the most recent shutdown and upgrade events, with the most recent shown first.	The log will display "unknown" if there has been an unexpected reboot or power failure or after an upgrade. If this occurs frequently, report the issues to customer support.

Diagnostic information

Field	Field description	Usage tips
Diagnostic information	Diagnostic files are provided in **.zip** archive format that contain a text document. To download a diagnostic file, click **Download file**.	Diagnostic information is provided to aid in troubleshooting problems that may occur with the TelePresence Server. In the event of an issue with the TelePresence Server, the support team may ask you for these diagnostic files.
Network capture file	To download a network capture, click **Download file**.	
System logs	To download the logs, click **Download file**.	An archive containing several useful log files.

Displaying hardware health status

The **Health status** page (**Status > Health status**) displays information about the hardware components of the TelePresence Server.

Note: The **Worst status seen** conditions are those since the last time the TelePresence Server was restarted.

To reset these values, click **Clear**. Refer to the table below for assistance in interpreting the information displayed.

Device health details

Field	Field description	Usage tips
Fans (7010 only) **Voltages** **RTC battery**	Displays two possible states: ■ OK ■ Out of spec States indicate both *Current status* and *Worst status seen* conditions.	The states indicate the following: ■ *OK* – component is functioning properly ■ *Out of spec* – Check with your support provider; component might require service If the *Worst status seen* column displays *Out of spec*, but *Current status* is *OK*, monitor the status regularly to verify that it was only a temporary condition.
Temperature	Displays three possible states: ■ OK ■ Out of spec ■ Critical States indicate both *Current status* and *Worst status seen* conditions.	The states indicate the following: ■ *OK* – temperature of the TelePresence Server is within the appropriate range ■ *Out of spec* – Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked ■ *Critical* – temperature of TelePresence Server is too high. An error also appears in the event log indicating that the system will shutdown in 60 seconds if the condition persists If the **Worst status seen** column displays *Out of spec*, but **Current status** is *OK* monitor the status regularly to verify that it was only a temporary condition.

Displaying cluster status for a master blade

To display cluster status, go to **Status > Cluster**.

Cluster status is only available for blades that are configured on the Cisco TelePresence Supervisor MSE 8050 to be part of a cluster. For more information about clustering, refer to Understanding clustering.

The table below describes the **Status > Cluster** page that displays for the master blade in a cluster. For details about slave blades, see Displaying cluster status for a slave blade.

Cluster status

Field	Field description	Usage tips
Slot	The number of the slot in the Cisco TelePresence MSE 8000 chassis that corresponds to this row in the table.	To configure a blade as a master or a slave in a cluster, log in to the Supervisor.
IP	The IP address of the blade in this slot, or *Master blade* (if this is the master).	

Field	Field description	Usage tips
Status	The status of the master blade can only be *OK* which means that this blade is operating correctly in the cluster. Possible statuses for a slave blade are: ■ *OK*: The master and slave are communicating correctly. ■ *OK (last seen <number> seconds ago)*: The master has lost contact with the slave. The slave will restart itself and in this way it will rejoin the cluster. Wait a few minutes and then refresh the **Status > Cluster** page. ■ *Still starting up*: The slave blade is in the process of starting up. Wait a few minutes and then refresh the **Status > Cluster** page. ■ *Lost contact <number> secs ago*: The master has lost contact with the slave. The slave will restart itself and in this way it will rejoin the cluster. Wait a few minutes and then refresh the **Status > Cluster** page. ■ *Cluster support not enabled*: There is no Cluster support feature key on this blade. ■ *Failed, version mismatch*: All blades in the cluster must be running the same version of software. This status message indicates that this blade is running different software to the master blade. This blade is not part of the cluster. Update all blades in the cluster to the same version of software. ■ *Blade not configured as slave*: The Supervisor has told the master that the blade is a slave, but the blade is not a slave. Possibly the slave blade was replaced. ■ *Blade incorrect type*: Possibly the slave blade was replaced with a different blade type after the cluster was configured.	If the status of the slave is OK, it is currently functioning in the cluster. For any of the other statuses, the slave blade is not currently functioning as part of the cluster. If a slave blade has a problem that causes it to no longer be part of the cluster, the cluster can continue to operate without that slave. For example, in a cluster of three blades if one slave fails, the master and the other slave can continue to operate and accept calls. There will just be fewer video ports available. Similarly, in a cluster of two blades, if the slave fails, the master continues to operate. If a slave blade fails, participants in conferences will not be disconnected: if there are sufficient resources on another blade in the cluster, they will continue to receive audio and video. In the worst case, the video will disappear, but the audio will continue because all audio is processed by the master blade. If the master loses contact with a slave, the slave will automatically restart itself. In this way, it can rejoin the cluster.
Media processing load	An overview of the current media loading of each blade in the cluster. The load may increase during periods of peak conference use.	Conferences are distributed between the blades in the cluster. The loads on the blades depend on the number of conferences running on each blade and the sizes of those conferences. On a slave blade, the audio load will always be zero: the master is responsible for all the audio.

Field	Field description	Usage tips
Screen licenses	The number of screen licenses on each blade in this cluster.	All screen licenses on slave blades are controlled by the master blade. Depending on how you use the blades in the MSE chassis, you might want to allocate all screen licenses to the slot that houses the master blade or you might distribute them between the slots in the cluster. It does not matter to the cluster how you have allocated the screen licenses—the master controls all screen licenses and even if a blade has failed in the cluster, the master will continue to have access to any screen licenses allocated to the failed blade's slot.

Displaying cluster status for a slave blade

To display cluster status, go to **Status > Cluster**. When you look at the **Status > Cluster** page on a slave blade, it shows the status of the master blade.

The table below describes the **Status > Cluster** page that displays for slave blades in a cluster. For information about the master blade, see Displaying cluster status for a master blade.

Slave blades have restricted user interfaces; not all settings are available. You must configure the cluster from the master blade.

Cluster status

Field	Field description	Usage tips
Status	Possible statuses for the master blade are: ■ *Still starting up*: the master blade is in the process of starting up. Wait a few minutes and then refresh the **Status > Cluster** page. ■ *OK*: The master and slave are communicating correctly. ■ *Lost contact*: The slave blade has lost contact with the master blade. This status will only be momentarily visible because the slave blade will quickly restart itself in this case.	If a slave blade loses contact with the master blade, it will restart itself. This is the only way that the slave blade can correctly rejoin the cluster. A common reason for a slave blade to lose contact with the master is because the master blade has restarted.
Last seen	This field is only visible if the master has not been seen for 11 seconds. The slave blade will automatically restart itself very soon after it loses contact with the master.	
IP address	The IP address of the master blade.	

Network settings

Configuring network settings

To configure the network settings on the TelePresence Server and check the network status, go to **Network > Network settings**.

On this page:

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the TelePresence Server. When you have finished, click **Update IP configuration** and then reboot the TelePresence Server.

IPv4 configuration

Field	Field description	Usage tips
IP configuration	Specifies whether the port should be configured manually or automatically. If set to *Automatic via DHCP* the TelePresence Server obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to *Manual* the TelePresence Server will use the values that you specify in the Manual configuration fields below.	Click **Renew DHCP** to request a new IP address if you have selected automatic configuration. You can disable IPv4 on the TelePresence Server port but only if logged in using IPv6.
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify this option if you have chosen *Manual* IP configuration, as described above. For Port A, if the IP configuration setting is set to *Automatic by DHCP* this setting will be ignored.
Subnet mask	The subnet mask required for the IP address you wish to use, for example 255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	

IPv6 configuration

Field	Field description	Usage tips
IP configuration	Select *Disabled*, *Automatic via SLAAC/DHCPv6* or *Manual*. If you select *Manual*, you must also supply the IPv6 address, prefix length and default gateway. If you select *Automatic via SLAAC/DHCPv6*, the TelePresence Server automatically gets an IPv6 address. It uses SLAAC, Stateful DHCPv6 or Stateless DHCPv6 as indicated by the ICMPv6 Router Advertisement (RA) messages (see Automatic IPv6 address preferences below).	Disable IPv6 on the port if the network does not support IPv6. You can disable IPv6 on the TelePresence Server port but only if logged in using IPv4.
IPv6 address	If you chose *Manual* configuration, supply the IPv6 address in CIDR format. Enclose the address in square brackets, for example `[fe80::202:b3ff:fe1e:8329]`, in the user interface.	You only need to enter an address if you chose *Manual* IP configuration. If you chose *Automatic via SLAAC/DHCPv6*, a manually entered setting is ignored.
Prefix length	If you chose *Manual* configuration, supply the prefix length.	The prefix length is the (decimal) number of bits that are fixed for this address.
Default gateway	(Optional) Supply the IPv6 address of the default gateway on this subnet.	The address may be global or link-local

IP status

The IP status section shows the current IP settings for this Ethernet port of the TelePresence Server, as follows, whether they were automatically or manually configured.

IPv4 settings:

- DHCP
- IP address
- Subnet mask
- Default gateway

IPv6 settings:

- DHCPv6
- IPv6 address
- IPv6 default gateway
- IPv6 link-local address

Ethernet configuration

Configure the Ethernet settings for this port of the TelePresence Server, and then click **Update Ethernet configuration**.

Ethernet configuration

Field	Field description	Usage tips
Ethernet settings	Select *Automatic* or *Manual*. If you select *Manual*, you must also supply the speed and duplex settings. Select *Automatic* if you want this Ethernet port to automatically negotiate its Ethernet settings with the connected device.	It is important that the devices at either end of the Ethernet connection have the same settings. That is, configure both devices to use automatic negotiation, or configure them both with the same fixed speed and duplex settings.
Speed	Set the connection's speed to *10 Mbit/s* or *100 Mbit/s*. Select automatic negotiation if you require a connection speed of *1000 Mbit/s*.	The connection speed setting must be the same for the ports at both ends of this connection.
Duplex	Set the connection's duplex mode to *Full duplex* or *Half duplex*.	The connection duplex setting must be the same for the ports at both ends of this connection. Full duplex mode allows simultaneous bidirectional transmission, while half duplex mode only allows bidirectional transmission that is not simultaneous.

Ethernet status

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether or not this Ethernet link is connected.	
Speed	The speed (*10*/*100*/*1000 Mbit/s*) of this Ethernet link.	This value is negotiated with the device to which this port is connected or based on your manual configuration.
Duplex	The duplex mode (*Full duplex* or *Half duplex*) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value can not be changed, it is for information only.
Packets sent	The total number of packets sent from this port (all TCP and UDP traffic).	This information can help you confirm that the TelePresence Server is transmitting packets into the network.
Packets received	The total number of packets received by this port (all TCP and UDP traffic).	This information can help you confirm that the TelePresence Server is receiving packets from the network.
Statistics:	More statistics for this port. ■ Multicast packets sent ■ Multicast packets received ■ Total bytes sent ■ Total bytes received ■ Receive queue drops ■ Collisions ■ Transmit errors ■ Receive errors	This information can assist you with diagnosing network issues, such as link speed and duplex negotiation issues.

Configuring DNS settings

Go to **Network > DNS** to check and change the DNS settings of the TelePresence Server.

Click **Update DNS configuration** to apply the new settings.

DNS settings

Field	Field description	Usage tips
DNS configuration	Select how you want the TelePresence Server to get its name server address. For example, if you select *Via Port A DHCPv6*, the device will automatically get a name server address using DHCP over the IPv6 network connected to Ethernet port A. If you select *Manual*, you must provide a name server address. You may also want to provide a secondary name server or domain name (DNS suffix).	The TelePresence Server does not allow you to automatically configure the name server address if you have set a static IP address on the selected interface. For example, if you select *Via Port A DHCPv4* here but have also selected *Manual* in the IPv4 configuration section of the **Port A settings** page, the TelePresence Server will warn you that no DNS servers will be configured.
Host name	Specifies a name for the TelePresence Server.	Depending on your network configuration, you may be able to use this host name to communicate with the TelePresence Server, without needing to know its IP address.
Name server	The IP address of the name server.	Required if you select the *Manual* name server preference.
Secondary name server	Identifies an optional second name server.	If an optional second name server is configured, the TelePresence Server may send DNS queries to either name server.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	Add a suffix if you want to use unqualified host names to refer to devices (instead of using IP addresses). For example, if the domain name (suffix) is set to *cisco.com*, then a request to the name server to look up the IP address of host *endpoint* will actually look up *endpoint.cisco.com*.

View DNS status

Use the DNS status fields to verify the current DNS settings for the TelePresence Server, including:

- Host name
- Name server
- Secondary name server
- Domain name (DNS suffix)

Configuring IP routes settings

You may need to set up one or more routes to control how IP traffic flows in and out of the TelePresence Server.

It is important that you create these routes correctly, or you may be unable to make calls or access the web interface.

To configure the route settings, go to **Network > Routes**.

On this page:

IP routes configuration

In this section you can control how IP packets should be directed out of the TelePresence Server. You should only change this configuration if you have a good understanding of the topology of the network(s) to which the TelePresence Server is connected.

Add a new IP route

To add a new route:

1. Enter the IP address of the target network, and the mask length that defines the range of addresses.
2. Select whether the traffic to those addresses will be routed via **Port A**'s default gateway or a **Gateway** that you specify.
3. Click **Add IP route**.
   The new route is added to the list. If the route already exists, or aliases (overlaps) an existing route, the interface prompts you to correct the route.

Use the following table for reference:

IP route configuration

Field	Field description	Usage tips
IP address / mask length	Use these fields to define the range of IP addresses to which this route applies. IPv4 addressing: Enter the IP address of the target network in dotted quad format, setting any unfixed bits of the address to 0. Use the **mask length** field to specify how many bits are fixed (and thus how many are unfixed, giving the range of addresses). IPv6 addressing: Enter the IP address of the target network in CIDR format, setting any unfixed bits of the address to 0. Use the **mask length** field to specify how many bits are fixed (and thus how many are unfixed, giving the range of addresses). Enclose any IPv6 addresses in square brackets.	IPv4 example: To route all IPv4 addresses in the range 192.168.4.128 to 192.168.4.255, specify the IP address as 192.168.4.128 and the mask length as 25. The first 25 bits are fixed, which means that the last seven bits determine the range of addresses. IPv6 example: To route all IPv6 addresses in the range 2001:db8::0000 to 2001:db8::ffff, enter the IP address 2001:db8:: and the mask length as 112. The first 112 bits are fixed, which means that the last 16 bits determine the range of addresses.
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	You may select *Port A*, or *Gateway*. If you select *Gateway*, enter the IP address of the gateway to which you want packets to be directed. If you select *Port A*, matching packets will be routed to Port A's default gateway (see Configuring network settings).

To view or delete an existing IP route

The page displays the following details for each route:

- The IP address pattern and mask
- Where matching packets will be routed, with the possibilities being:
  - Port A—meaning the default gateway configured for Port A
  - **<**IP address**>**—a specific address has been chosen
- Whether the route has been configured automatically as a consequence of other settings, or manually added by you.

The *default* routes are configured automatically by your choice of *Default gateway preference*s for IPv4 and IPv6 (see Configuring network settings) and cannot be deleted. Any packets destined for addresses that are not matched by your manually configured routes will be routed via the default gateway.

You can delete manually configured routes. Select the check boxes next to the routes then click **Delete selected**.

Current routes tables

Each table shows all configured routes (both manual and automatic) for IPv4 and IPv6 for the TelePresence Server's Ethernet port. If you want to change the IP configuration for the Ethernet port, go to **Network > Network settings**.

Configuring IP services

To configure IP services, go to **Network > Services**.

Use this page to allow or deny access to the listed web services on the TelePresence Server. Refer to the table below for more details.

The TelePresence Server offers web services, such as HTTP for the web interface and H.323 for making and receiving calls. You can control which services may be accessed on the unit's Ethernet interfaces and the TCP/UDP ports through which those services are available.

Check the boxes next to the service names, edit the port numbers if necessary, and then click **Apply changes**.

If you want to reset the values to their default settings, click **Reset to default** and then click **Apply changes**.

Note: the options shown on this page will be for IPv4 and/or IPv6 depending on which IP versions are enabled on the **Network > Network settings** page.

TCP service

Field	Field description	Usage tips
Web	Enable/disable web access on the appropriate port.	Web access is required to view and change the TelePresence Server web pages and read online help files. If you disable web access on Port A you will need to use the serial console interface to re-enable it.
Secure web	Enable/disable secure (HTTPS) web access on the specified interface or change the port that is used for this service.	This field is only visible if the TelePresence Server has the *Encryption* feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the TelePresence Server. By default, the TelePresence Server has its own SSL certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates.
Incoming H.323	Enable/disable the ability to receive incoming calls to the TelePresence Server using H.323 or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to H.323 devices being made by the TelePresence Server.
SIP (TCP)	Allow/reject incoming calls to the TelePresence Server using SIP over TCP or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the TelePresence Server.
Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the TelePresence Server using SIP over TLS or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the TelePresence Server.

Field	Field description	Usage tips
FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	FTP can be used to upload and download TelePresence Server configuration. You should consider disabling FTP access on any port that is outside your organization's firewall. If you require advanced security for the TelePresence Server, disable FTP access.

UDP service

Field	Field description	Usage tips
SIP (UDP)	Allow/reject incoming and outgoing calls to the TelePresence Server using SIP over UDP or change the port that is used for this service.	Disabling this option will prevent calls using SIP over UDP.

Configuring QoS settings

To configure Quality of Service (QoS) on the TelePresence Server for audio and video, go to **Network > QoS**.

QoS is a term that refers to a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize audio transmissions and video transmissions over HTTP traffic. These settings affect all outgoing audio and video packets. All other packets are sent with a QoS of 0.

The TelePresence Server allows you to set a 6-bit value for Type of Service (IPv4) or Traffic Class (IPv6), which can be interpreted by networks as either Type of Service (ToS) or Differentiated Services (DiffServ). Note that in terms of functionality, IPv6 QoS is identical to IPv4 QoS.

CAUTION: Do not alter the QoS settings unless you need to do so.

To configure the QoS settings you need to enter a 6-bit binary value.

Further information about QoS, including values for ToS and DiffServ, can be found in the following RFCs, available on the Internet Engineering Task Force web site www.ietf.org:

- RFC 791
- RFC 2474
- RFC 2597
- RFC 3246

On this page:

About QoS configuration settings

The tables below describe the settings on the **Network > QoS** page.

Click **Update QoS settings** after making any changes.

IPv4 configuration

Field	Field description	Usage tips
Audio	Six bit binary field for prioritizing audio data packets on the network.	Do not alter this setting unless you need to.
Video	Six bit binary field for prioritizing video data packets on the network.	Do not alter this setting unless you need to.

IPv6 configuration

Field	Field description	Usage tips
Audio	Six bit binary field for prioritizing audio data packets on the network.	Do not alter this setting unless you need to.
Video	Six bit binary field for prioritizing video data packets on the network.	Do not alter this setting unless you need to.

ToS configuration

ToS configuration represents a tradeoff between the abstract parameters of precedence, delay, throughput, and reliability.

ToS uses six out of a possible eight bits. The TelePresence Server allows you to set bits 0 to 5, and will place zeros for bits 6 and 7.

- Bits 0-2 set IP precedence (the priority of the packet).
- Bit 3 sets delay: 0 = normal delay, 1 = low delay.
- Bit 4 sets throughput: 0 = normal throughput, 1 = high throughput.
- Bit 5 sets reliability: 0 = normal reliability, 1 = high reliability.
- Bits 6-7 are reserved for future use and cannot be set using the TelePresence Server interface.

You need to create a balance by assigning priority to audio and video packets whilst not causing undue delay to other packets on the network. For example, do not set every value to 1.

DiffServ configuration

DiffServ uses six out of a possible eight bits to set a codepoint. (There are 64 possible codepoints.) The TelePresence Server allows you to set bits 0 to 5, and will place zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

Default settings

The default settings for QoS are:

- **Audio** *101110*:
  - For ToS, this means IP precedence is set to 5 giving relatively high priority. Delay is set to low, throughput is set to high, and reliability is set to normal.
  - For Diff Serv, this means expedited forwarding.
- **Video** *100010*:
  - For ToS, this means IP precedence is set to 4 giving quite high priority (but not quite as high as the audio precedence). Delay is set to normal, throughput is set to high, and reliability is set to normal.
  - For DiffServ, this means assured forwarding (codepoint 41).

To return the settings to the default settings, click **Reset to default**.

Configuring SSL certificates

If the Cisco TelePresence Server has the *Secure management (HTTPS)* or *Encryption* feature key installed, and you enable *Secure web* on the **Network > Services** page, you will be able to access the web interface of the TelePresence Server using HTTPS.

Note: A certificate and key are also required if you select to use the SIP TLS service in **Network > Services**.

The Cisco TelePresence Server has a local certificate and private key pre-installed and it uses this to authenticate itself to the browser when you access the unit using HTTPS. However, Cisco recommends that you upload your own certificate and private key to ensure security because all Cisco TelePresence Server's have identical default certificates and keys.

The TelePresence Server uses DTLS to negotiate encryption parameters with TIP endpoints—this requires a certificate to be used. The TelePresence Server's implementation of DTLS handles customer-supplied certificates in the following way:

- Opportunistic DTLS always uses the default certificate for DTLS negotiation, even if a customer-supplied certificate is uploaded.
- Negotiated DTLS uses the customer-supplied certificate if one is uploaded (this is the preferred procedure).

Negotiated DTLS will be used if the endpoint supports RFC 5763; otherwise, in a TIP call, opportunistic DTLS will be attempted.

To upload your own certificate and key, go to **Network > SSL certificates**. Complete the fields using the table below for help and click **Upload certificate and key**. Note that you must upload a certificate and key simultaneously. You must restart the Cisco TelePresence Server after uploading a new certificate and key.

Note: A certificate and private key must be in PEM format.

You can remove your own certificate and key, if necessary, by clicking **Delete custom certificate and key**.

The following table details the fields on the **Network > SSL certificates** page:

Local certificate

Field	Field description	Usage tips
Subject	The details of the business to which the certificate has been issued: ■ **C**: the country where the business is registered. ■ **ST**: the state or province where the business is located. ■ **L**: the locality or city where the business is located. ■ **O**: the legal name of the business. ■ **OU**: the organizational unit or department. ■ **CN**: the common name for the certificate, or the domain name.	
Issuer	The details of the issuer of the certificate.	Where the certificate has been self-issued, these details are the same as for the **Subject**.

Field	Field description	Usage tips
Issued	The date on which the local certificate was issued.	
Expires	The date on which the local certificate will expire.	
Private key	Whether the private key matches the certificate.	Your web browser uses the SSL certificate's public key to encrypt the data that it sends back to the Cisco TelePresence Server. The private key is used by the Cisco TelePresence Server to decrypt that data. If the **Private key** field shows 'Key matches certificate' then the data is securely encrypted in both directions.

Local certificate configuration

Field	Field description	Usage tips
Certificate	If your organization has bought a certificate, or you have your own way of generating certificates, you can upload it. Click **Choose File** to find and select the certificate file.	A certificate and private key must be in PEM format.
Private key	Click **Choose File** to find and select the private key file that accompanies your certificate.	A certificate and private key must be in PEM format.
Private key encryption password	If your private key is stored in an encrypted format, you must enter the password here so that you can upload the key to the Cisco TelePresence Server.	

Trust store

Field	Field description	Usage tips
Subject	The details of the trust store certificate; usually a certificate issued by the authority that is used to verify the local certificate.	
Issuer	The details of the issuer of the trust store certificate.	These are the details of the trusted certification authority.
Issued	The date on which the trust store certificate was issued.	
Expires	The date on which the trust store certificate will expire.	

Trust store configuration

Field	Field description	Usage tips
Trust store	The trust store is required for two reasons: ■ to verify the identity of the remote end of a SIP TLS connection (incoming call or outgoing call or registration) ■ to verify the identity of the remote end of an outgoing HTTPS connection (e.g. feedback receivers or API applications calling **`participant.diagnostics`**)	Browse to and select the trust store certificate file, then click **Upload trust store**. The store may contain multiple certificates. When verification is required (see following setting) the certificate of the remote party is verified against the trust store: the remote certificate must either be in the trust store or in the trust chain of one of its certificates. Click **Delete trust store** if you need to remove it or replace it with an updated file.
Certificate verification settings	Determines the circumstances in which the remote certificate must be verified with the trust store.	Select one of the drop-down options below and click **Apply changes**. ■ *No verification*: The remote certificate is never verified against the trust store (remote end always trusted). ■ *Outgoing connections only*: The TelePresence Server attempts to verify the remote certificate for all outgoing SIP TLS and HTTPS connections. ■ *Outgoing connections and incoming calls*: The TelePresence Server attempts to verify the remote certificate for all incoming and outgoing SIP TLS connections, and for outgoing HTTPS connections.

Testing network connectivity

You can use the **Network connectivity** page to troubleshoot network issues between the TelePresence Server and a remote video conferencing device (host).

On this page you can ping another device from the TelePresence Server's web interface and trace the route to that device. The results show whether or not you have network connectivity between the TelePresence Server and the remote host.

To test connectivity with a remote device, go to **Network > Connectivity**. In the text box, enter the IP address or hostname of the device to which you want to test connectivity and click **Test connectivity**.

The results show the outbound interface for the query and the IP address of the remote host.

The ping results show the roundtrip time in milliseconds and the TTL (Time To Live) value on the echo reply.

For each intermediate host (typically routers) between the TelePresence Server and the remote host, the host's IP address and response time are shown.

Not all devices will respond to the messages from the TelePresence Server. Routing entries for non-responding devices are shown as <*unknown*>. Some devices are known to send invalid ICMP response packets (for example, with invalid ICMP checksums). Invalid ICMP responses are also not recognized by the TelePresence Server so these responses are also shown as <*unknown*>.

Note: The ping message is sent from the TelePresence Server to the IP address of the remote host. Therefore, if the TelePresence Server has an IP route to the given host, the ping will be successful. This feature allows the TelePresence Server's IP routing configuration to be tested, and it has no security implications.

Note: If you are unable to ping the remote host, then check your network configuration—especially any firewalls using NAT.

Configuration

Configuring system settings

The **System settings** page allows you to control settings of the TelePresence Server configured conference settings.

To access this information, go to **Configuration > System settings**.

To update the default, or change the configuration at any time, edit the field referring to the table below for details and click **Apply changes**.

Note Endpoints and conferences assume the values you provide here. These settings apply to all calls and conferences on the unit and are not configurable elsewhere.

Setting for all configured conferences

Field	Field description	Usage tips
Display video preview images	When checked, thumbnail preview images of conference participants' video streams are shown on the TelePresence Server user interface.	The default is enabled (checked).

Configuring H.323 settings

The H.323 settings page allows you to enable the TelePresence Server to use an H.323 gatekeeper.

To access this information, go to **Configuration > H.323 settings**.

To update the defaults, or change the configuration at any time, edit the fields referring to the table below for details and click **Apply changes**.

H.323 gatekeeper

Field	Field description	Usage tips
Use gatekeeper	Enables the TelePresence Server to register numeric IDs for its conferences with an H.323 gatekeeper. Check the box to enable this feature.	When disabled, no gatekeeper registrations are attempted (and existing registrations are removed), regardless of other gatekeeper or per-conference settings. When enabled, registrations with the gatekeeper are attempted, and the gatekeeper is contacted for incoming and outgoing calls. If the gatekeeper does not respond, calls are still connected if possible.
Address	The network address of the gatekeeper to which TelePresence Server registrations should be made.	Can be specified either as a host name or as an IP address. This field will have no effect if **Use gatekeeper** is disabled.
H.323 ID to register	Specifies a server-wide identifier that the TelePresence Server can use to register itself with the H.323 gatekeeper.	The TelePresence Server must make a server-wide registration before it can register any IDs with the H.323 gatekeeper. This field is required for the gatekeeper registration, but has no effect if **Use gatekeeper** is disabled.
Password	If the configured gatekeeper requires password authentication from registrants, enter the password.	The password is used, in association with the **H.323 ID to register** as the username, to authenticate the TelePresence Server to the gatekeeper (only if the gatekeeper is configured to require authentication).

Configuring SIP settings

The SIP settings page allows you to control the TelePresence Server SIP settings.

To access this information, go to **Configuration > SIP settings**.

To update the defaults, or change the configuration at any time, edit the fields referring to the table below for details and click **Apply changes**.

SIP

Field	Field description	Usage tips
Outbound call configuration	This setting affects outgoing SIP calls and registration. The options are: *Use trunk* disables SIP registration and tears down existing registrations. Routes outbound calls to the trunk destination, e.g. VCS or CUCM. *Call direct* disables SIP registration and tears down existing registrations. Outbound SIP calls go directly (not via trunk).	*Use trunk*: ■ Directs outbound SIP calls via the trunk to the SIP server address you provide. ■ The SIP server, for example Cisco Video Communication Server (VCS) or Cisco Unified Call Manager (CUCM), is responsible for the onward routing of outbound SIP calls from the TelePresence Server. *Call direct*: ■ The TelePresence Server will connect SIP calls directly if possible. It does not use the **Outbound address** or **Outbound domain** parameters. ■ The TelePresence Server does not attempt to use the trunk.
Outbound address	The hostname or IP address of the trunk destination.	The TelePresence Server ignores this field if **Outbound call configuration** is set to *Call direct*.
Outbound domain	The domain of the trunk destination.	The TelePresence Server ignores this field if **Outbound call configuration** is set to *Call direct*. The TelePresence Server uses this value for any outbound SIP calls where the supplied address does not contain an @ symbol. If you do not specify an outbound domain, the TelePresence Server uses the outbound address instead.
Username	The TelePresence Server uses this name to authenticate with the SIP device (trunk destination or endpoint) if that device requires authentication.	
Password	The TelePresence Server uses this password to authenticate with the SIP device (trunk destination or endpoint) if that device requires authentication.	The SIP destination may not require authentication; if it does, you need to configure it to accept a log in from this username and password combination.

Field	Field description	Usage tips
Outbound transport	Select the protocol that the TelePresence Server will use for outbound calls. One of *TCP*, *UDP*, or *TLS*.	The TelePresence Server uses this protocol for communicating with the trunk destination. If you have the encryption feature key installed and want to encrypt signaling, select *TLS*. The TelePresence Server accepts incoming connections on whichever protocol the connection uses (TCP, UDP or TLS), and will respond using the same protocol, irrespective of this **Outbound transport** setting. Make sure that you enable those services on the **Network > Services** page.
Negotiate SRTP using SDES	Select whether the TelePresence Server will negotiate SRTP using SDES for either of the following options: ■ *for secure transports (TLS) only* ■ *for all transports*. (Note this parameter only displays with the encryption feature key.)	The TelePresence Server supports the use of encryption with SIP. When encryption is in use with SIP, the audio and video media are encrypted using Secure Real-time Transport Protocol (SRTP). When using SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDES). SDES exchanges keys in clear text, so it is a good idea to use SRTP in conjunction with a secure transport for call control messages. You can configure the TelePresence Server to also use Transport Layer Security (TLS) which is a secure transport mechanism that can be used for SIP call control messages. The default setting is *for secure transports (TLS) only*.
Use local certificate for outgoing connections and registrations	Check this option to allow the TelePresence Server to present its local certificate when making outgoing TLS calls. With this option unchecked, the TelePresence Server will never present its local certificate, even if requested to do so.	This option should be checked if TLS is in use.

Operation mode

The Operation mode page allows you to define the operation mode of the TelePresence Server, that is, whether to allow it to be locally managed or remotely managed by a device such as Cisco TelePresence Conductor.

When the TelePresence Server is set to remotely managed mode its resources can be optimized dynamically. This means that calls can connect and only use the resources they require, giving the most efficient use of blade resources across the different media types (i.e. audio, video, content) of different participants.

To set the operation mode, go to **Configuration > Operation mode**.

To add or change the Operation mode at any time, edit the field referring to the table below for details and click **Apply changes**.

Caution:

- Changing the operation mode requires the TelePresence Server to be rebooted.
- In remotely managed mode, configured endpoints and conferences are not available.
- Any conferences configured on the TelePresence Server in remotely managed mode are lost when the unit reboots.

The two operation modes are supported by two separate APIs. When using remotely managed mode the Flexible API is operational and when using locally managed mode the Standalone API is operational.

For more information on using the APIs please refer to Cisco TelePresence Server 3.0 API Reference Guide.

Operation mode setting

Field	Field description	Usage tips
Operation mode	This selection determines the operation mode for the TelePresence Server. The options are: ■ *Locally managed* ■ *Remotely managed*	In locally managed mode the TelePresence Server will manage all conferences. In remotely managed mode all conference create and participant management are managed externally to the TelePresence Server, by a device such as Cisco TelePresence Conductor and so resources will be optimized dynamically. Default is locally managed mode.

Displaying and resetting system time

You can manually set the system date and time for the TelePresence Server or let it use the Network Time Protocol (NTP) to synchronize its time.

To configure Time settings, go to **Configuration > Time**.

System time

Current time displays the time according to the TelePresence Server.

To manually set the system date and time, type the new values and click **Change system time**.

NTP

The TelePresence Server supports the NTP protocol. If you want the TelePresence Server to automatically synchronize with an NTP server, enter the NTP settings and then click **Update NTP settings**.

The TelePresence Server synchronizes with the NTP server every hour.

If the NTP server is local to either of the TelePresence Server's enabled Ethernet interfaces, the TelePresence Server automatically uses the port to communicate with the NTP server.

If the NTP server is not local, the TelePresence Server will use the port that is configured as the default gateway to communicate with the NTP server, unless a specific IP route to the NTP server's network/IP address is specified (see **Network > Routes**).

If there is a firewall between the TelePresence Server and the NTP server, configure the firewall to allow NTP traffic to UDP port 123.

Device time settings

Field	Field description	Usage tips
Enable NTP	Check the box to enable NTP protocol on the TelePresence Server.	
UTC offset	The offset of the time zone that you are in from UTC.	You must manually update this offset to account for regional changes to time zone, such as British Summer Time and other daylight saving schemes.
NTP host	The IP address or hostname of the server that is acting as the time keeper for the network.	

Using NTP over NAT (Network Address Translation)

No extra configuration is required if the NAT is local to the TelePresence Server's network.

If NAT is used on the NTP server's local network, you must configure the NAT forwarding table to forward NTP data from the TelePresence Server to UDP port 123 on the NTP server.

Backing up and upgrading the TelePresence Server

On this page:

Upgrading the main TelePresence Server software image

The main TelePresence Server software image is the only firmware component that you will need to upgrade.

To upgrade the main TelePresence Server software image:

1. Go to **Configuration > Upgrade**.
2. Check the **Current version** of the main software image to verify the currently installed version.
3. Log onto the support pages to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the TelePresence Server web browser interface.
7. Go to **Configuration > Upgrade**.
8. Click **Browse** to locate the unzipped file on your hard drive.
9. Click **Upload software image**. The browser begins uploading the file to the TelePresence Server, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
10. The upgrade status displays in the **TelePresence Server software upgrade status** field.
11. Shut down and restart the TelePresence Server.

Upgrading the loader software image

Typically, upgrades for the loader software image are not available as often as upgrades to the main software image.

Note: You should not do this unless you are advised by customer support.

To upgrade the loader software image:

1. Go to **Configuration > Upgrade**.
2. Check the **Current version** of the loader software to verify the currently installed version.
3. Go to the software download pages of the web site to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.

6. In the web interface, click the button to locate and select the unzipped file on your hard drive.
7. Click **Upload software image**. The browser begins uploading the file to the TelePresence Server, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Loader image upgrade completed."
8. The upgrade status displays in the **Loader upgrade status** field.
9. Shut down and restart the TelePresence Server.

Backing up and restoring the configuration

The Back up and restore section of the **Configuration > Upgrade** page allows you to back up and restore the configuration of the TelePresence Server using the web interface. This enables you to either go back to a previous configuration after making changes or to effectively clone a unit by copying its configuration to another.

To back up the configuration, click **Save backup file** and save the resulting configuration.xml file to a secure location.

To restore configuration at a later date:

1. Click **Browse** to locate and select a previously-saved configuration.xml file.
2. Select whether you want the saved configuration to overwrite the current *Network settings*, *User settings*, or both.
   The overwrite controls are not selected by default; the software assumes you want to preserve existing network settings and user accounts.
3. Click **Restore backup file**.

When restoring a new configuration file to a TelePresence Server you can control which parts of the configuration are overwritten:

- If you check **Network settings**, the network configuration will be overwritten with the network settings in the supplied file.
  Typically, you would only select this check box if you are restoring from a file backed up from the same TelePresence Server or if you are intending to replace an out of service TelePresence Server.
  If you copy the network settings from a different, active, TelePresence Server and there is a clash (for instance, both are now configured to use the same fixed IP address) one or both devices may become unreachable via IP. If you do not check **Network settings**, the restore operation will not overwrite the existing network settings, with the one exception of the QoS settings. QoS settings are overwritten regardless of the **Network settings** check box.
- If you check **User settings**, the current user accounts and passwords will be overwritten with those in the supplied file.
- If you overwrite the user settings and there is no user account in the restored file corresponding to your current login, you will need to log in again after the file has been uploaded.

Enabling TelePresence Server features

The TelePresence Server requires activation before most of its features can be used. (If the TelePresence Server has not been activated, the banner at the top of the web interface will show a prominent warning; in every other respect the web interface will look and behave normally.)

If this is a new TelePresence Server it should already be activated; if it is not, or if you have upgraded to a newer firmware version, or if you are enabling a new feature, contact your supplier to obtain the appropriate activation code.

Each activation code is unique to a particular TelePresence Server. Ensure that you know the blade's serial number when you request the code, so that the supplier can give you the correct code.

Regardless of whether you are activating the TelePresence Server or enabling an advanced feature, the process is the same.

Additionally, if it is a Cisco TelePresence Server 7010, then the port licence key is also entered here.

To activate the TelePresence Server or enable an advanced feature:

1. Read the **Activated features** list to check whether the feature you require is already activated. Product activation is also in this list, which shows feature names and activation keys.
2. Enter the code given to you by your supplier into the **Activation code** field *exactly as you received it*, including any dashes.
3. Click **Update features**.
   The browser window refreshes to list the newly activated feature and the code you entered.
   If the activation code is not valid, you are prompted to re-enter it.
   Activation codes may be time-limited. If this is the case, an expiry date will be displayed, or a warning that the feature has already expired. Expired activation codes remain in the list but the corresponding features are not activated.
4. Record the activation code in case you need to re-enter it in the future.

Successful TelePresence Server or feature activation has immediate effect and will persist even if the TelePresence Server is restarted.

Note that you can remove some types of features. Click **remove**, next to the feature key, to remove a feature.

Upgrading the font

Your TelePresence Server may be shipped with the TrueType font pre-installed. You can check this on the **Status** or **Configuration > Upgrade** pages.

If the font is not present, and you want to use TrueType text rendering on your TelePresence Server instead of the default text rendering method, you must upload the font file which is supplied by your TelePresence Server vendor:

Note: You should do this when the TelePresence Server is not heavily loaded. Also, you must use the supplied font; do not attempt to load a different font file.

1. Click **Browse** to locate and select your font file.
2. Click **Upload font**.
   The **Font file status** changes to *Present*.

Downgrade the font

1. If you want to revert to the default text rendering, click **Delete font**.
2. Confirm that you want to remove the font file.

The **Font file status** changes to *Not present*.

Shutting down and restarting the TelePresence Server

You may need to shut down the TelePresence Server to restart it as part of an upgrade or to switch off its power.

Caution: Shutting down the TelePresence Server will disconnect all active calls.

To shut down the TelePresence Server:

1. Go to **Configuration > Shutdown**.
2. Click **Shut down TelePresence Server**.
   The button changes to **Confirm TelePresence Server shutdown**.
3. Click the button again to confirm.
   The TelePresence Server will begin to shut down. The banner at the top of the page will change to indicate this.
   When the shutdown is complete, the button changes to **Restart TelePresence Server**.
4. Click this button a final time to restart the TelePresence Server.

Changing the administrator password

This page allows you to change the administrator password used to log in to this TelePresence Server. This applies to the current user who needs to be an 'administrator'. To access this page, go to **Configuration > Change password.**

We recommend that you change the administrator password regularly. You may want to make a note of the password and store it in a secure location.

To change the password, type in the new password twice and click **Change password**.

Backing up and restoring the configuration via FTP

You can back up and restore the configuration via the web interface of the TelePresence Server or via FTP. You need to have the FTP service enabled on the TelePresence Server (on the **Network > Services** page) before you can connect to it using FTP.

To back up the configuration via FTP:

1. Connect to the TelePresence Server using an FTP client and the administrator credentials you use to log in to the web interface.
   You will see a file called **configuration.xml** that contains the configuration of your TelePresence Server.
2. Download this file and store it somewhere safe.

To restore the configuration using FTP:

1. Locate the copy of **configuration.xml** that you want to restore.
2. Connect to the TelePresence Server using an FTP client and the administrator credentials you use to log in to the web interface.
3. Upload your **configuration.xml** file to the TelePresence Server, overwriting the existing version of the file.

Note: The same process can be used to transfer a configuration from one TelePresence Server blade to another. However, before doing this, be sure to keep a copy of the original feature keys from the blade whose configuration is being replaced.

If you are using the configuration file to configure a duplicate blade, be aware that you will need to reconfigure any static IP addresses on the duplicate blade(s).

Conferences

Displaying the conference list

The **Conferences** page lists all the conferences that are configured on this TelePresence Server, regardless of their status (e.g. *Active* or *Inactive*).

Go to **Conferences** to access this list.

Conferences are sorted alphabetically by name by default. To change sort order, or sort the list by Status or URI instead, click the relevant column heading.

On this page you can:

- Delete conferences.
- Click a conference name to display its status.

The list contains the following information for each conference:

Conference list details

Field	Field description	Usage tips
Name	The name of the pre-configured conference.	Click the conference name to display conference status and participants.
URIs	The URI(s) assigned to the conference.	In remotely managed mode the TelePresence Server does not register individual conference URIs to a gatekeeper. Conferences can have up to 2 multi-use URIs which participants can dial. If the URI is PIN protected this status will be shown. Individual participants can have their own URI(s) which they dial. These are not displayed in this list.

Field	Field description	Usage tips
Status	The status of the conference: ■ *Scheduled* ■ *Active* ■ *Inactive* This field may also display warnings about the conference's configuration.	Conferences can be: ■ A *Scheduled* conference shows the time until the start of the conference. ■ An *Active* conference displays *(<X> endpoints, <N> screens)* or *Active (<X> endpoints)* if all endpoints are audio-only). ■ An *Inactive* conference is effectively the same as an *Active* one but it has no participants. However, it can have URIs, time until the start and durations. The status may have additional information about the conference duration, and whether it is locked. For example, *Inactive - Ends in 5 hours and 27 minutes [Locked]*. Conference configuration warnings may be displayed, for example: *[No participants allowed - limited to 0 participants]*.

Displaying conference status

A conference's **Status** page displays the live status of the conference. Go to **Conferences** then click a conference name to see the **Status** page.

From this page you can tell whether the conference:

- is active and how many endpoints are in the conference
- is locked
- includes a content channel
- has participants and the status of each
- had previous participants and who they were
- has URI(s) assigned to the conference

On the Conference > *Conference Name* > Status page you can:

- Select and then **Disconnect selected** participants
- **Disconnect all** participants, effectively ending the conference
- Send a message to one or all endpoints
- Click **More...** to see additional status information for a participating endpoint, or click **Expand all** to see this information for all active endpoints (see the following table for more details)

Conference status reference

Status

Field	Field description	Usage tips
Status	The status of the conference: ■ *Scheduled* ■ *Active* ■ *Inactive* This field may also display warnings about the conference's configuration.	Conferences can be: ■ A *Scheduled* conference shows the time until the start of the conference. ■ An *Active* conference displays *(<X> endpoints, <N> screens)* or *Active (<X> endpoints)* if all endpoints are audio-only). ■ An *Inactive* conference is effectively the same as an *Active* one but it has no participants. However, it can have URIs, time until the start and durations. The status may have additional information about the conference duration, and whether it is locked. For example, *Inactive - Ends in 5 hours and 27 minutes [Locked]*. Conference configuration warnings may be displayed, for example: *[No participants allowed - limited to 0 participants]*.
URI	The URI(s) assigned to the conference.	In remotely managed mode the TelePresence Server does not register individual conference URIs to a gatekeeper. Conferences can have up to 2 multi-use URIs which participants can dial. If the URI is PIN protected this status will be shown. Individual participants can have their own URI(s) which they dial. These are not displayed in this list.
Conference lock status	Indicates whether the conference is locked.	
Content	Whether the content channel is currently in use.	One of: ■ *No current presentation:* content sharing is enabled for the conference but there is no active contributor ■ *Presentation from <endpoint display name>*: there is an active contributor of content For more information, see Content channel support.

All participants

Field	Field description	Usage tips
Endpoint	The names of the endpoints currently participating in the active conference.	If the conference is not active, this section shows *No endpoints*. To remove a participant from the conference: select the appropriate check box and select **Disconnect selected** Click on the endpoint's name to go to its **Status** page.
Type	The endpoint type.	
Status	The status of the endpoint.	One of: ■ *Joining conference* - the endpoint is joining this conference ■ *In conference* - the endpoint is currently participating in this conference. ■ *Attempting to re-establish call* - the endpoint is busy and a retry is occurring. Additional status information may be displayed, for example, *xx failed to join*.(grouped endpoints), *packet loss detected*, *video to muted*, *video from muted*, *video muted* (and the equivalent for audio), *important* and *audio-only*. If a pre-configured endpoint is busy when the conference starts, the TelePresence Server will retry the endpoint up to five times throughout the conference and connect it if it becomes free. The retry intervals are 5, 15, 30, 60 and 120 seconds.
More...	Click **More...** to see previews of the transmit and receive streams. You can also control the endpoint's contribution to the conference. Click **[Expand / Collapse All]** to show more status information for all endpoints in the list.	You can: mute  and unmute  audio mute  and unmute  video make a participant important (transmit stream only)  or unimportant 

Previous participants

Field	Field description	Usage tips
Endpoint	The names of endpoints that were previously in this conference.	To reconnect participants to the conference: select the appropriate check boxes and select **Retry connection**. Click on the endpoint's name to go to its **Status** page.
Type	The endpoint type.	

Field	Field description	Usage tips
Reason for disconnection	Why the endpoint is no longer part of the conference.	The TelePresence Server may have disconnected the endpoint for one of the following example reasons: ■ *requested by administrator*: the endpoint has been disconnected by an administrator ■ *call rejected*: the far end rejected the call. ■ *left conference*: the endpoint has been disconnected at the end of a conference ■ *requested via API*: the endpoint has been disconnected via the API ■ *no answer*: the endpoint did not answer the call ■ *busy*: the endpoint has failed to connect because it was busy (for SIP calls this could also mean that the endpoint rejected the call). ■ *gatekeeper error*: a gatekeeper error occurred whilst trying to establish call. ■ *destination unreachable* The endpoint was unreachable. ■ *DNS failure*: DNS lookup failed, or the H.323 gatekeeper could not find the alias requested. ■ *Encryption not supported by far end*: encryption required for the call but the far end does not support it or encryption forbidden for this call but far end can not do unencrypted [to be updated] ■ *timeout*: Connection timed out. ■ *insufficient free ports*: the endpoint has been disconnected because there are insufficient free ports ■ *conference port limit reached*: the endpoint has been disconnected because the conference port limit has been reached ■ *Conference locked*: the call could not connect to the conference as it is locked. ■ *Product not activated*: the call could not be made/accepted as there is no activation key installed on the TelePresence Server. ■ *Protocol error*: the endpoint has been disconnected due to a protocol error ■ *Network error*: the endpoint has been disconnected due to a network error ■ *Unavailable*: the endpoint is unavailable ■ *Capability negotiation error*: the endpoint and the TelePresence Server are unable to negotiate a mutually compatible call set up.

Field	Field description	Usage tips
		■ *Insufficient token allocation*: the token specification/allocation was not sufficient for TIP/MUX call. ■ *TIP/MUX negotiation failure*: the endpoint has been disconnected because TIP/MUX negotiation failed to complete successfully. ■ *unspecified error*: the endpoint has disconnected, but the TelePresence Server does not know the reason

Users

Displaying the user list

The **Users** page provides an overview of all the user accounts that exist on the TelePresence Server.

User list details

Field	Field description
User ID	The user name needed to access the web interface of the TelePresence Server. You can enter text in whichever character set you require, however, note that some browsers and FTP clients do not support Unicode characters.
Name	The name of the user (optional, so may not be present).
Privilege	The access privileges associated with this user. Either *administrator* or *none*.
User attributes	Displays the access privilege level granted to this user: blank (full access) or *API access*. This field is always blank for *administrator* users, who also always have full access to the API, irrespective of the API setting. If you grant *API access* to a non-administrator account, that account can *only* access the API. This allows you to authorize applications that work with the TelePresence Server. You can create a user that has neither API access nor administrator privileges, but such a user can not log in and can not use the API.

Deleting users

Select the users and then click **Delete selected users**. You cannot delete the *admin* user.

Adding and updating users

You can add, edit and delete user accounts on the TelePresence Server by accessing the list of users (go to **Users**.)

Most of the information that you use when adding or editing user accounts is identical; any differences are explained in the following reference table.

Adding a user

1. Go to **Users**.
2. Click **Add new user**.
3. Supply the user account details, referring to the following table if necessary.
4. Click **Add user**.

Updating a user

1. Go to **Users**.
2. Click a User ID.
3. Modify the user account details, referring to the following table if necessary.
4. Click **Modify user**.
5. If you need to change the password, click **Change password**.

User details reference

User details

Field	Field description	More information
User ID	Identifies the log-in name or ID number of the user. This value is the username required to access the TelePresence Server.	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.
Name	The name of the user.	Optional.
Password	The required password, if any.	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters. Note that this field is only active when adding a new user. If you are updating an existing user and want to change that user's password, click **Change password** instead.
Administrator	Select this check box to make this user an Administrator.	Administrators have complete control of the TelePresence Server — they can change any aspect of the TelePresence Server's configuration, and can schedule and modify conferences.
API access	Select this check box to allow this user account to be used by applications that communicate with the TelePresence Server via API commands.	

Logs

Working with the event logs

If you are experiencing complex issues that require advanced troubleshooting, you may need to collect information from the TelePresence Server logs. Typically, you will be working with customer support who can help you obtain these logs.

Event log

The TelePresence Server stores the 2000 most recently captured messages generated by its sub-systems. It displays these on the **Event log** page (**Logs > Event log**). In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log.

Customer support can interpret logged messages and their significance for you if you are experiencing a specific problem with the operation or performance of your TelePresence Server.

You can:

- Click the column headers to sort the events.
- Click the page numbers to jump through the displayed log in steps of 100 events.
- Download the log as text: go to **Logs > Event log** and click **Download as text**.
- Change the parameters of the display to limit the information to your area of interest (**Logs > Event display filter**).
- Change the level of detail collected in the traces by editing the **Event capture filter** page.

Note: Only modify the event capture filter if instructed to do so by customer support. Modifying these settings can impair the performance of your TelePresence Server.

- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Syslog** page.
- Empty the log by clicking **Clear log**.

Note: Only modify the event capture filter if instructed to do so by customer support. Modifying these settings can impair the performance of your TelePresence Server.

Event capture filter

The event capture filter defines which events the TelePresence Server will keep in the log. By default this filter is configured to capture *Errors, warnings and information* from all the TelePresence Server sub-systems.

Note: Only modify this filter if doing so with advice from Customer Support.

For example, when troubleshooting a TelePresence Server issue, a support representative may ask you to capture detailed trace for the video sub-system:

1. Go to **Logs > Event capture filter**.
2. Select *Detailed trace* from the **VIDEO** drop-down list.
   The TelePresence Server warns you that performance may be affected.
3. Click **OK** (this is a temporary elevation in detail that you can reverse after your issue is resolved).
4. Click **Update settings**.
   The TelePresence Server will capture detailed trace information from the video sub-system, as well as the default information for all other sub-systems.

Event display filter

You can use the event display filter to view a subset of the event log or highlight particular entries. This filter works on stored entries, it does not affect which events are captured.

To modify the event display filter, go to **Logs > Event display filter**.

Text filtering

1. Enter a **Filter string** to display only the stored events that contain that string.
2. Enter a **Highlight string** if you want to easily see the string within the filtered results.
3. Click **Update display**.
   The TelePresence Server displays the filtered and highlighted event log.

Display levels

There are many sub-systems of the TelePresence Server which can all log events. You can modify the level of detail you want to see for each sub-system or for all sub-systems.

For example, if you were only interested in SIP errors:

1. Scroll to the bottom of the page where you can see the **Set all to:** button and the dropdown next to it.
2. Select *None* on the dropdown.
3. Click **Set all to:**.
   The display level changes to *None* for all sub-systems.
4. Select *Errors only* from the dropdown next to the SIP sub-system.
5. Click **Update settings**.
   The TelePresence Server displays only SIP errors.

Logging H.323 or SIP messages

The **H.323/SIP log** page records every H.323 and SIP message received by or transmitted from the TelePresence Server.

The H.323/SIP log is disabled by default because the volume of messages affects performance, but Customer Support may ask you to enable it to assist in troubleshooting.

Click **Enable H323/SIP logging** to start recording these protocol messages. You can also **Download as XML** for further processing or to send to support.

When you are satisfied that the issue is resolved, you should **Disable H323/SIP logging** and then **Clear log** to avoid impacting the performance of the unit in future.

Logging using syslog

You can send the Event log to one or more syslog servers on the network for storage or analysis.

To configure the syslog facility, go to **Logs > Syslog**.

Syslog settings

Refer to this table for assistance when configuring Syslog settings:

Syslog settings

Field	Field description	Usage tips
Host address 1 to 4	Enter the IP addresses of up to four Syslog receiver hosts.	The number of packets sent to each configured host will be displayed next to its IP address.
Facility value	A configurable value for the purposes of identifying events from the Cisco TelePresence Server on the Syslog host. Choose from the following options: ■ *0 - kernel messages* ■ *1 - user-level messages* ■ *2 - mail system* ■ *3 - system daemons* ■ *4 - security/authorization messages (see Note 1)* ■ *5 - messages generated internally by syslogd* ■ *6 - line printer subsystem* ■ *7 - network news subsystem* ■ *8 - UUCP subsystem* ■ *9 - clock daemon (see Note 2)* ■ *10 - security/authorization messages (see Note 1)* ■ *11 - FTP daemon* ■ *12 - NTP subsystem* ■ *13 - log audit (see Note 1)* ■ *14 - log alert (see Note 1)* ■ *15 - clock daemon (see Note 2)* ■ *16 - local use 0 (local0)* ■ *17 - local use 1 (local1)* ■ *18 - local use 2 (local2)* ■ *19 - local use 3 (local3)* ■ *20 - local use 4 (local4)* ■ *21 - local use 5 (local5)* ■ *22 - local use 6 (local6)* ■ *23 - local use 7 (local7)*	Choose a value that you will remember as being the Cisco TelePresence Server. **Note 1:** Various operating system daemons and processes utilize Facilities 4, 10, 13 and 14 for security/authorization, audit and alert messages which seem to be similar. **Note 2:** Various operating systems utilize both Facilities 9 and 15 for clock (cron/at) messages. Processes and daemons that have not been explicitly assigned a Facility value may use any of the "local use" facilities (16 to 21) or they may use the "user-level" facility (1) - and Cisco recommend that you select one of these values.

Using syslog

The events that are forwarded to the syslog receiver hosts are controlled by the event log capture filter.

To define a syslog server, enter its IP address and then click **Update syslog settings**. The number of packets sent to each configured host is displayed next to its IP address.

Note: Each event will have a severity indicator as follows:

- 0 - Emergency: system is unusable (unused by the Cisco TelePresence Server)
- 1 - Alert: action must be taken immediately (unused by the Cisco TelePresence Server)
- 2 - Critical: critical conditions (unused by the Cisco TelePresence Server)
- 3 - Error: error conditions (used by Cisco TelePresence Server *error* events)
- 4 - Warning: warning conditions (used by Cisco TelePresence Server *warning* events)
- 5 - Notice: normal but significant condition (used by Cisco TelePresence Server *info* events)
- 6 - Informational: informational messages (used by Cisco TelePresence Server *trace* events)
- 7 - Debug: debug-level messages (used by Cisco TelePresence Server *detailed trace* events)

Working with Call Detail Records

The TelePresence Server can display up to 2000 Call Detail Records. However, the TelePresence Server is not intended to provide long-term storage of Call Detail Records. If you wish to retain CDR logs, you must download them and store them elsewhere.

When the CDR log is full, the oldest logs are overwritten.

To view and control the CDR log, go to **Logs > CDR log**. Refer to the tables below for details of the options available and a description of the information displayed.

Call Detail Record log controls

The CDR log can contain a lot of information. The controls in this section help you to select the information for display that you find most useful. When you have finished making changes, click **Update display** to make those changes take effect. Refer to the table below for a description of the options:

CDR log controls

Field	Field description	Usage tips
Messages logged	The current number of CDRs in the log.	
Filter records	The list of CDR record types that the TelePresence Server logs.	Leave the boxes blank to display all records, or check the boxes of the record types you are interested in.
Filter string	Use this field to limit the scope of the displayed Call Detail Records. The filter string is not case-sensitive.	The filter string applies to the **Message** field in the log display. If a particular record has expanded details, the filter string will apply to these as well.
Expand details	By default, the CDR log shows only brief details of each event. When available, select from the options listed to display more details.	Selecting *All* will show the greatest amount of detail for all messages, regardless of which other options are selected.

Call Detail Record log

The Call Detail Record log displays as a long table which may span multiple pages and includes up to 2000 rows. In addition to the filtering described above, you can navigate the log in the following ways:

- To sort ascending or descending by any of the columns, click the column header.
- To filter the log for all records related to a particular conference or participant GUID, click the GUID (click **Show all** to reverse this filter).
- To jump to a particular page in the displayed list of records, click the page number.

Click **Download as XML** to process the log in your text editor, or archive it for future reference. This button *downloads all the records* currently stored; it ignores any display filters you have set on the web page.

Note: Avoid downloading CDR logs when the unit is under heavy load; performance may be impaired.

Click **Clear all records** to empty the log memory.

Caution: Clear all records *permanently removes all records* from the TelePresence Server. You cannot retrieve cleared records.

CDR log reference

The following table describes the fields in the CDR log:

CDR log details

Field	Field description	Usage tips
# (record number)	The unique index number for this Call Detail Record.	
Time	The time at which the Call Detail Record was created.	Records are created as different conference events occur. The time the record was created is the time that the event occurred. Incoming CDR log events are stored with the local time stamp (not UTC). Changing the time (either by changing the system time or via an NTP update) causes new events in the CDR log to show the new time. No change will be made to the timestamp of existing records.
Conference	The GUID of the conference to which this record applies.	Each new conference is created with a globally unique identifier (GUID). All records relating to a particular conference display this identifier, which can make auditing conference events much simpler. Click the GUID to see only those records that relate to this conference.
Participant	The GUID of the participant to which this record applies.	Each participant is represented by a globally unique identifier (GUID), which can simplify your record management. Click the GUID to see only those records that pertain to this participant.
Message	The type of the Call Detail Record, and brief details, if available.	Click **>>** to expand the details of all messages of this type. You can do this for all messages by selecting *All* and clicking **Update display**, which can be useful in combination with the **Filter string** to find records where the message contains a particular word.

API clients

The TelePresence Server logs the ten most recent API clients that have made requests to the unit. To see this list, click **Logs > API clients**.

Clients that have not made an API request for more than five minutes will appear greyed out.

Click **Refresh** to update the list of API clients. To clear all data, click **Reset statistics**. This clears the current list of API clients. As clients send new commands, they will reappear in this list.

By default the page is sorted by the **Time since last request** column.

API client details

Field	Field description	Usage tips
Client IP	The IP address of the client sending the request.	
Time since last request	The time since the last request was sent by that client.	
Last request method	The last API request method sent by that API client.	
Last request user	The username that the client used in their API request.	Clients whose last API request failed authentication will be flagged up here with *(authentication failed)*.
Requests received since last reset	The number of requests received since the last reset.	If more than one request is received per second then the average number of requests per second is displayed in (). The current threshold is 1.8 requests per second. 'Overactive' clients are only flagged up if they are currently communicating with the TelePresence Server. The elapsed time since the last reset is shown below the table, beside the buttons.

Feedback receivers

The TelePresence Server publishes feedback events so that any receivers listening to it can take action when something changes. To see the list of feedback receivers, click **Logs > Feedback receivers**.

You can clear all configured feedback receivers by clicking **Delete all**. You cannot undo this action.

Each receiver in the list has the following details:

Feedback receiver details

Field	Field description	Usage tips
Index	The position of the receiver in the list of receivers.	
Receiver URI	The fully qualified URI of the receiver.	The receiver may be a software application, for example Cisco TelePresence Management Suite, that can respond to the feedback events with an appropriate API call to retrieve the list of changes from the feedback source.

Reference

Content channel support

Most telepresence endpoints support the use of a second video channel known as the content channel. Typically this is used for presentations running alongside live video.

- H.323 systems use a protocol called H.239 to receive and send the content channel video.
- SIP systems use a protocol called BFCP for content.
- Cisco CTS systems and other TIP systems use TIP to control content sharing.

The TelePresence Server caters for endpoints that do not support the second video channel by allowing content in main video. When this feature is enabled the TelePresence Server sends the content in the main video channel to those endpoints. The content channel is composed with the normal video while the content channel is active (content is displayed in the largest pane and other participants' video streams are centered continuous presence panes across the bottom of the display).

For more information please refer to the Cisco TelePresence Server 3.0 API Reference Guide.

Understanding how participants display in layout views

Note: These options are not configurable from the TelePresence Server user interface if the TelePresence Server is operating in remotely managed mode.

On this page:

Conference layouts

The layout chosen by the TelePresence Server for a system depends on the number of screens that the system has and the characteristics of the other conference participants. Single-screen endpoints can also choose a layout with far end camera control or can be preconfigured to one of the choices below. The TelePresence Server is capable of working with one-, two-, three- and four-screen regular and immersive endpoints, and displaying any combination of those systems participating in a conference to any other type of system in the conference.

In general, the behavior of the TelePresence Server is to display the "loudest" participants in the most prominent layout panes. If there are more contributors than there are panes available, then the "quietest" participants are not shown.

Layouts sent to single-screen systems

The default layout can be configured either boxwide or per participant. This default setting can be overridden by a participant changing the layout selection using far end camera control or via DTMF keys 2 and 8.

In ActivePresence layout, the loudest participant appears full screen with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen.

The ActivePresence layout is possible when the other participants in the conference are all single-screen endpoints, or a mixture of single-screen endpoints and multiple-screen systems that reveal which camera has the loudest audio input (the Cisco TelePresence TX9000 for example).

Only the Equal layout can be sent if there are any multi-screen systems not supporting loudest participant information. The ActivePresence, Single and Prominent layouts all rely on that information.

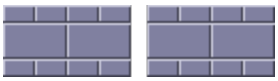
The TelePresence Server composes the layout for single-screen endpoints according to the setting of the **Default layout type for single-screen endpoints**:

Layouts sent to single-screen endpoints

	*Single*: Endpoints will be shown in one full screen pane.
	*ActivePresence*: Endpoints will be shown in one full screen pane with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen.
	*Prominent*: Endpoints will be shown in one large pane with additional participants appearing in up to four equally sized panes at the bottom of the screen.
	*Equal*: Endpoints will be shown in a grid pattern of equally sized panes on the screen, up to 4x4. Each row of panes can either show screens of a remote multi-screen system or a combination of remote systems with fewer screens.

Layouts sent to two-screen systems

Layouts sent to two-screen systems

	If there are any three- or four-screen TelePresence systems in a conference, the TelePresence Server sends this layout to two-screen systems in that conference. Each row of four panes can either show the four screens of a remote four-screen system or a combination of systems with fewer screens.
	If there are only one- and two-screen systems in the conference, the TelePresence Server uses this layout (if all of the video streams to show fit into the available panes). The overlaid panes (maximum of four) are automatically centered if possible.

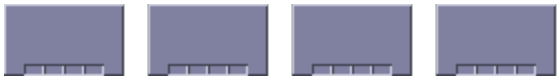
Layouts sent to three-screen systems

Layouts sent to three-screen systems

	If there are any four-screen TelePresence systems in a conference, the TelePresence Server sends this layout to three-screen systems in that conference. The central row of four large panes can either show the four screens of a remote four-screen system or a combination of one-, two- and three-screen conference participants. In order for this row to be correctly centered, the TelePresence Server shows the panes in the center of the three screens and does not use the left side of the leftmost screen or the right side of the rightmost screen.
	If there are no four-screen TelePresence systems in a conference, the TelePresence Server uses this layout for three-screen systems in that conference. The TelePresence Server uses this layout if all of the participants to be shown will fit within the available continuous presence panes. The overlaid panes are automatically centered if possible.
	If there are no four-screen TelePresence systems in a conference, the TelePresence Server uses this layout for three-screen systems in that conference. The TelePresence Server uses this layout if it needs more small continuous presence panes to show participants. The TelePresence Server automatically switches between this layout and the previous one as participants leave and join the conference.

Layout sent to four-screen systems

The TelePresence Server sends this layout to four-screen systems in a conference:



Each row of four panes (the row consisting of the four full-screen panes or one of the rows of four small overlaid panes) can either show a four-screen system or a combination of remote systems with fewer screens. The overlaid panes are automatically centered if possible.

OneTable mode

A TelePresence Server in OneTable mode contributes three different video streams of the participants in the call, and therefore the TelePresence Server no longer displays the three streams received from these systems side by side in three adjacent panes.

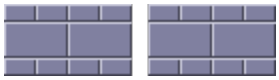
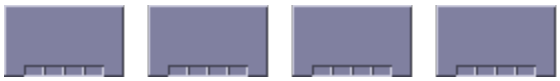
To enable OneTable mode, go to the configuration page of the conference and set **Use OneTable mode when appropriate** to *4 person mode*.

4 person mode: The TelePresence Server composes the participant video streams as if there were four people sitting next to each other on one side of a table, irrespective of their physical location.

The conference must have at least three participants present that support the OneTable feature.

The conference layout sent to connected systems varies based on how many screens those systems have as follows:

OneTable mode layouts

	Layout sent to single-screen systems. The overlaid panes are automatically centered if possible.
	Layout sent to two-screen systems.
	Layout sent to three-screen systems. The overlaid panes are automatically centered if possible.
	Layout sent to four-screen systems. The overlaid panes are automatically centered if possible.

Endpoint configuration options that affect view layouts

Self view setting

The **Self view** setting for an endpoint determines whether the TelePresence Server ever displays its own video stream on that endpoint; that is, whether a participant may see himself/herself. If this setting is not selected, the endpoint will never display its own video stream.

If you do allow an endpoint to display its own video then the TelePresence Server always places the self view last when placing participants in the available view panes, even if the participant is one of the loudest in the call (i.e. even if he or she is shown prominently to the other conference participants).

Show full screen view of single-screen endpoints

When placing participants within layout panes, the TelePresence Server places the "loudest" people first, in the most prominent panes, and the quietest people in the smaller panes. However, in conferences with a mixture of TelePresence systems (which typically use large, high resolution, displays) and systems capable of much lower quality video (for example, video-capable cellphones) it is not always desirable for the lower-resolution participants to be shown in the large full screen panes.

For single screen systems, the **Show full screen view of single-screen endpoints** setting determines whether an endpoint is ever allowed to be shown in a large full-screen pane.

If this option is not selected, the endpoint will never be shown full screen to other conference participants, even if it is one of the loudest speakers in the conference. If this option is selected, the endpoint will be shown full screen when it is one of the active speakers in the conference.

This setting is not displayed for multi-screen endpoints and endpoint groups.

Minimum screen layout setting

As described above, when choosing which conference layout to send to a participant the TelePresence Server takes into account the number of screens used by other participants in the conference. For example, the following layout is sent to single screen systems if there are any four screen systems in the conference:

The **Minimum screen layout** allows you to influence the layout used either because of personal preference or to avoid dynamic changes during the conference (for example, if you know that a four-screen endpoint will join the conference at some point, then using the *4 screens wide* setting tells the TelePresence Server to choose layouts based on its presence even before it has connected).

The default setting — *Auto detect* — causes the TelePresence Server to apply the choices described above based on the actual number of screens in use by the conference participants.

However, a setting of *3 screens wide* or *4 screens wide* causes the TelePresence Server to apply the layout choices described above based on the actual number of screens used by the conference participants **and** the virtual presence of a three- or four-screen endpoint. For example, *4 screens wide* would provide the following layout to all single screen endpoints in the conference even if all of the current participants are using single screen systems.

Equally, if you select a setting of *3 screens wide* and a four-screen endpoint joins the conference, the view will change to the one above.

Allow content in main video

This feature allows the TelePresence Server to send a conference's content in the main video channel of endpoints that do not support the extra channel and would otherwise be unable to see the content.

The content channel stream is given the largest pane of this composed layout, which is shown in the main video channel. The continuous presence panes of up to four other participants are composed across the bottom of the layout below the content stream. The continuous presence panes are centered.

Show borders around endpoints setting

If **Show borders around endpoints** is enabled, the TelePresence Server draws borders around participants that are displayed in small panes; it does not draw borders around participants being shown in full-screen panes.

The TelePresence Server draws a red border around the active speaker in the conference, and a white border around other participants. There may not always be an active speaker to highlight in a conference, for example if everyone is muted or no-one is talking.

Enabling this setting for an endpoint means that the video layout sent to that endpoint will use borders; it does not mean that this participant will always be shown within a border to other participants – those other participants' views will use their own **Show borders around endpoints** setting.

Marking a participant as "important"

For each conference, one active participant can be set as "important". This means that the TelePresence Server considers this participant first when deciding which contributors to show in which layout panes, rather than their position in the list being set by how loudly they are speaking. See the endpoint control settings in Displaying conference status.

Muted participants

Audio mute

Participants who have had their audio muted from the web interface do not contribute audio to the conference. Additionally, muted participants are considered after participants who are not muted when the TelePresence Server places participants in view layout panes.

Note that other participants will not have an indication that a participant has been muted. They simply will no longer hear that participant speaking.

Video mute

Participants who have had their video muted from the web interface do not contribute video to the conference. They will continue to contribute audio as normal, unless it is muted separately.

Endpoint types

Endpoint types

Endpoint type (shown in UI)	Hardware names / model numbers
Standard	Standard video endpoints, for example: ■ Cisco TelePresence Movi (software endpoint) ■ Microsoft OCS (software endpoint) ■ Cisco TelePresence System MXP Series (1700 MXP, 1000 MXP) Also displays if the endpoint type is unknown to the TelePresence Server
TANDBERG T1 or TANDBERG single screen TelePresence	Cisco TelePresence System T1 (formerly TANDBERG Telepresence T1)
TANDBERG T3 or TANDBERG three screen TelePresence	Cisco TelePresence System T3 (formerly TANDBERG Telepresence T3)
Group of N endpoints	A group of endpoints. The list does not contain the individual group members
TIP endpoint	An unknown type of Cisco CTS system, running legacy software (CTS 1.6 / 1.7 up to 1.7.3)
TIP endpoint	A Cisco CTS single screen system, running legacy software (CTS 1.6 / 1.7 up to 1.7.3) for example: ■ CTS 500 ■ CTS 1000 ■ CTS 1100
TIP endpoint	A Cisco CTS three screen system, running legacy software (CTS 1.6 / 1.7 up to 1.7.3) for example: ■ Cisco TelePresence System 3000 series (CTS 30x0) ■ Cisco TelePresence System 3200 series (CTS 32x0)
SIP telepresence	An unknown type of Cisco CTS or other TIP-capable system running CTS 1.7.4 or later
SIP single screen telepresence	A Cisco CTS or other TIP-capable single screen system running CTS 1.7.4 or later, for example: ■ CTS 500 ■ CTS 1000 ■ CTS 1100
SIP three screen telepresence	A Cisco CTS or other TIP-capable three screen system running CTS 1.7.4 or later, for example: ■ Cisco TelePresence System 3000 series (CTS 30x0) ■ Cisco TelePresence System 3200 series (CTS 32x0)

Endpoint interoperability

Endpoint feature support

Feature	Endpoints that support this	Notes
Reveal loudest participant for panel switched layout	T3, CTS 3200, CTS 3000, TX9000, TX9200	CTS 1300 and endpoint groups do not reveal the loudest participant.
Add legacy TIP endpoint	■ CTS 500 ■ CTS 1000 ■ CTS 1100 ■ CTS 1300 ■ CTS 3000 ■ CTS 3010 ■ CTS 3200 ■ CTS 3210	You must add these endpoints using **Add legacy TIP endpoint** if they are running versions 1.6.x or 1.7.x (up to and including 1.7.3) of the CTS software. You may be able to add these endpoints using **Add new endpoint** if they are running CTS software versions 1.7.4 or higher.
Conference ending notification	■ CTS 500 ■ CTS 1000 ■ CTS 1100 ■ CTS 1300 ■ CTS 3000 ■ CTS 3010 ■ CTS 3200 ■ CTS 3210 ■ TX9000 ■ TX9200	These endpoints generate their own conference ending warning when they receive notification from the TelePresence Server. They show an icon instead of an overlaid message as seen by other types of endpoints.
OneTable mode	T3	If several participants in the conference are using these endpoints, and if OneTable mode is enabled, then the TelePresence Server will use the OneTable layout mode.

Understanding clustering

A cluster is a group of blades, hosted on the same Cisco TelePresence MSE 8000 chassis, that are linked together to behave as a single unit. You can configure and manage clusters using the Cisco TelePresence Supervisor MSE 8050.

A cluster provides the combined screen count of all the blades in the cluster. This larger screen count provides you with the flexibility to set up conferences with more participants or several smaller conferences.

Overview of a Cisco TelePresence Server MSE 8710 cluster

Cisco TelePresence Server MSE 8710 blades running software version 2 or later support clustering. Currently you can cluster up to four blades, with one blade being the master and the others being slaves.

Clustering provides you with the combined video port count of the blades in the cluster. For example, on a cluster of four blades, each with 12 screen licenses, the cluster has 48 video ports. The master can allocate them as necessary, for example, all in one large conference, or distributed across several smaller conferences. See port allocations for more information.

Master blades

The screen licenses allocated to all the blades in a cluster are "inherited" by the master blade; all ports in the cluster are controlled by the master. Therefore, after you have configured a cluster, you must control functionality through the master using either its web interface or through its API. All calls to the cluster are made through the master.

Slave blades

Slave blades do not display the full blade web interface. Only certain settings are available, such as network configuration, logging and upgrading. Similarly, a slave blade will only respond to a subset of API calls. For more information, refer to the relevant API documentation.

Upgrading clustered blades

If you need to upgrade the blades in a cluster, first upload the new software images to each blade in the cluster and then restart the master. The slaves will automatically restart and the upgrade will be completed.

General points

Some points to note about clustering:

- If you want to cluster a blade, the blade must have the cluster support feature key.
- The Supervisor must be running software version 2.1 or above to configure clustering.
- You may only cluster identical blades; they must be of the same type and must be running the same version of their software.
- You can have more than one cluster in a chassis and the chassis can host different types of clusters.

- Blades that do not support clustering can be installed into an MSE 8000 chassis alongside a cluster.
- You must assign the cluster roles (master/slave) to the slots in the chassis; if a blade fails, you can replace it and the cluster configuration will persist; however, the active calls and conferences are affected as follows:
  - If you restart or remove the master, the slaves will also restart: all calls and conferences end.
  - If a slave blade fails, the clustering configuration on the Supervisor and the blade may disagree. In this case, the Supervisor pushes the clustering configuration to the blade. The clustering configuration only includes clustering information; it does not configure network settings or anything else on the blade. If the Supervisor has pushed a configuration change to a blade, the Supervisor will prompt you to restart the blade.
  - If the Supervisor restarts or is removed, the cluster continues to function, conferences continue, and the cluster does not restart when the Supervisor reappears.
- Always keep a recent backup of the Supervisor.
- You cannot upload / delete the enhanced font file on a slave blade; it is only required by the master.

Getting help

If you experience any problems when configuring or using Cisco TelePresence Server, see the "Product documentation" section of these release notes. If you cannot find the answer you need in the documentation, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

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.