Cisco TelePresence TelePresence Server 8710 and 7010 2.2

Product user guide

D14842

June 2011

Contents

Introduction

Welcome to the Cisco TelePresence Server product user guide.

This document accompanies version 2.2 of the TelePresence Server software. 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.

System status

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.	
System log	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. If this occurs frequently, report the issues to customer support.
H.323 gatekeeper status	How many TelePresence Servers are registered to an H.323 gatekeeper, and whether the registrations have been made to the primary or an alternate gatekeeper.	This field is only displayed on the Conference controller TelePresence Server and on the master blade in a TelePresence Server cluster.
SIP registrar status	How many TelePresence Servers are registered to a SIP registrar.	This field is only displayed on the Conference controller TelePresence Server and on the master blade in a TelePresence Server cluster.
Conference control	Whether this TelePresence Server is the Conference controller.	Can be: ■ *Conference controller - this system will manage all conferences* ■ *Conferences will be managed by an external controller* For more information, see Understanding the conference controller.

Field	Field Description	Usage tips
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.

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.
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. It also activates the grouped endpoints and rooms features.	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, endpoint groups, and the rooms feature. 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.
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. For more information about licenses, see Understanding screen licenses. Screen licenses are shared between the Conference controller TelePresence Server and the TelePresence Servers it controls. For a Conference controller TelePresence Server, the value shown is the total number of screen licenses for all controlled TelePresence Servers.

Conference status

Field	Field description	Usage tips
Active TelePresence Servers	If this TelePresence Server is the Conference controller then this field shows the number of TelePresence Servers (including this system) that are being controlled by this TelePresence Server.	A TelePresence Server that is not the Conference controller will show 0 here. For more information, see Understanding the Conference controller.

Field	Field description	Usage tips
Active conferences	The number of active conferences that this TelePresence Server is controlling.	If this is the Conference controller, then this is the number of active conferences across all managed TelePresence Servers. A TelePresence Server that is not the Conference controller will show 0 here. For more information, see Understanding the Conference controller.
Active endpoints	The number of endpoints (of all types) that are in active conferences controlled by this TelePresence Server.	If this is the Conference controller, then this is the number of endpoints in active conferences across all managed TelePresence Servers. A TelePresence Server that is not the Conference controller will show 0 here. For more information, see Understanding the Conference controller.
Video ports	The number of video ports in use. The second number is the maximum on this TelePresence Server.	If this is the Conference controller, the numbers are those across all managed TelePresence Servers controlled by this TelePresence Server. A TelePresence Server that is not the Conference controller will show 0 here. For more information, see Understanding the Conference controller and Content channel video support.
Audio ports	The number of audio-only ports in use. The second number is the maximum on this TelePresence Server.	
Content ports	The number of content channel ports in use. The second number is the maximum 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. 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**.	The network capture file is only available on the master blade in a TelePresence Server cluster.
System logs	To download the logs, click **Download file**.	An archive containing several useful log files.

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.

Note: The Conference controlling arrangement is not the same as the clustering arrangement of multiple TelePresence Servers. For more information, see Comparing clustering with Conference controlling.

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; in any case, 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.

Note: The Conference controlling arrangement is not the same as the clustering arrangement of multiple TelePresence Servers. For more information, see Comparing clustering with Conference controlling.

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.	

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
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.

Network settings

Configuring network settings

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

The TelePresence Server has two Ethernet interfaces, Port A and Port B. However, Port B is for future expansion and cannot be enabled in the current release of the TelePresence Server. Therefore, although there is a **Network > Port B settings** page, you cannot change any settings for Port B.

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. Port A should never be disabled because it is the primary interface of the TelePresence Server.
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.
IP 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.	You can not change this value, 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.

DNS settings

Click **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). **Note:** Although *Port B* appears in this dropdown, you should not select it because it is disabled in this version of the software.	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.	(Optional) The TelePresence Server queries the secondary DNS server if the primary is unavailable. If the first server is available but does not know an address, the TelePresence Server does not query the secondary DNS 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:

Port preferences

If both Ethernet ports are enabled, it is necessary to specify which port is used in certain special circumstances. Make the appropriate selections described below. Click **Apply changes**.

Default gateway preferences

Field	Field description	Usage tips
IPv4 gateway preference	Select the port whose default gateway setting the TelePresence Server will use to send IPv4 traffic in the absence of more specific routing (see IP routes configuration). The TelePresence Server routes IPv4 packets to the IPv4 default gateway when it does not have a more specific route. Therefore you only need one default IPv4 gateway, even though you may have configured *different* IPv4 default gateways on the TelePresence Server's ports.	If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference. If you select Port B as the default gateway preference, and then disable Port B, the TelePresence Server default gateway preference will revert to Port A.
IPv6 gateway preference	Select the port whose default gateway setting the TelePresence Server will use to send IPv6 traffic in the absence of more specific routing (see IP routes configuration). The TelePresence Server routes IPv6 packets to the IPv6 default gateway when it does not have a more specific route. Therefore you only need one default IPv6 gateway, even though you may have configured *different* IPv6 default gateways on the TelePresence Server's ports.	If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference. Selecting Port B as default gateway preference then disabling Port B will cause the preference to revert to Port A.

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, **Port B**'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*, *Port B* 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). If you select *Port B*, matching packets will be routed to Port B's default gateway. If Ethernet Port B is disabled, the option to route packets to Port B will be disabled.

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
  - Port B - meaning the default gateway configured for Port B
  - **<**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 Port preferences) 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**.

Routes behavior with disabled ports

If the default gateway preference is set to Port B but that port is disabled, the default route will automatically update to route unrecognised addresses via Port A.

If a manually configured route specifies Port B's default gateway but that port is disabled, packets matching that route **will be discarded**. They will not be automatically routed via Port A. You must take care to avoid this situation.

Current routes table

This table shows the IPv4 and IPv6 default gateways for each of the TelePresence Server's Ethernet ports. If you want to change the default gateways for the Ethernet ports, go to **Network > Port A** or **Network > Port B**.

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**.

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. If a port is disabled, this option will be unavailable.
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. If a port is disabled, this option will be unavailable.
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. If a port is disabled, this option will be unavailable.
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. If a port is disabled, this option will be unavailable.

Field	Field description	Usage tips
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. If a port is disabled, this option will be unavailable.
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. If a port is disabled, this option will be unavailable.

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. If a port is disabled, this option will be unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B.

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 audio and video packets to H.323 endpoints. 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.

Note: 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.

Field	Field description	Usage tips
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 Cisco 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, we recommend that you upload your own certificate and private key to ensure security because all Cisco TelePresence Servers have identical default certificates and keys.

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.

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**.
Issued	The date on which the local certificate was issued.	
Expires	The date on which the local certificate will expire.	

Field	Field description	Usage tips
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.	
Private key	Click **Choose File** to find and select the private key file that accompanies your certificate.	
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: ■ *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. Click **Apply changes**.

Network connectivity testing

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

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, regardless of whether that route lies out of port A or port B, 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

System settings

The System settings page allows you to control a number of aspects of the TelePresence Server status:

- whether it is the Conference controller
- whether to use a gatekeeper
- some global conference settings

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

Note 1: Endpoints and conferences inherit the values you provide here by default. If you change a local setting to something other than the inherited value, the local setting always takes precedence over the system-wide setting.

Note 2: Changes to configuration in the Default conference settings and New endpoint default settings sections do not affect active calls — to change these settings for an active call use the Advanced settings and Configuration pages for the appropriate endpoint.

Conference control

Field	Field description	Usage tips
Conference control	Choose from: ▪ *Conference controller - this system will manage all conferences* ▪ *Conferences will be managed by an external controller*	Select an option from the drop-down list. For more information, see Understanding the Conference controller.

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.

Field	Field description	Usage tips
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.

SIP

Field	Field description	Usage tips
Outbound call configuration	This setting affects outgoing SIP calls and registration. There are three options: *Use registrar* enables SIP registration and routes outbound SIP calls via the registrar. *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 registrar or trunk).	*Use registrar*: Enables SIP registrations, on a system-wide basis, with the registrar address you provide. Outgoing calls always go through the registrar, unless you explicitly choose **Call direct** for a pre-configured endpoint or ad hoc call. An outbound call will fail if the registrar does not respond. Incoming calls should come through the registrar and will fail if the registrar does not respond. *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**, **Outbound domain**, or **Outbound transport** parameters. The TelePresence Server does not attempt to use either the registrar or trunk.
Outbound address	The hostname or IP address of the SIP registrar or trunk destination.	The TelePresence Server ignores this field if **Outbound call configuration** is set to *Call direct*.

Field	Field description	Usage tips
Outbound domain	The domain of the SIP registrar or trunk destination.	The TelePresence Server ignores this field if **Outbound call configuration** is set to *Call direct*. The TelePresence Server uses this value in the following ways: ■ **`username`*`@outbounddomain`*** to register a user with a SIP registrar (if SIP registration is enabled) ■ **`numericId`*`@outbounddomain`*** to register a conference's numeric ID with a SIP registrar (if conference has SIP registration enabled) ■ 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 if it registers with a SIP registrar. In the case where multiple TelePresence Servers are controlled by one, the others register the same name with numerical suffixes (e.g. **`_2`**, **`_3`**). The TelePresence Server uses this name to authenticate with the SIP device (registrar, trunk destination, or endpoint) if that device requires authentication.	The TelePresence Server will use this name to register itself with the SIP registrar if you have enabled SIP registration. It won't register itself if you don't provide this, but it will still be able to register individual conferences (assuming they are enabled to register and have numeric IDs). If a conference does not have a numeric ID, then it cannot register. Calls out from such a conference will appear to come from the TelePresence Server's own SIP registration (**`this_username@outbounddomain`**). It is impossible for a participant to call into such a conference because it does not have a numeric ID. If you enter a full URI here (e.g. **`host@domain`**), then the TelePresence Server will ignore the **Outbound domain** setting.
Password	The TelePresence Server uses this password to authenticate with the SIP device (registrar, 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 (and registrations, if enabled). One of *TCP*, *UDP*, or *TLS*.	The TelePresence Server uses this protocol for communicating with the SIP registrar or 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.
Use local certificate for outgoing connections and registrations	Select this option to force the TelePresence Server to present its local certificate when registering with the SIP registrar (via TLS) or making outgoing TLS calls.	Only applies if TLS is used for outgoing calls and registrations (if enabled). The destination may not require the local certificate. You should only check this option if your environment dictates that the destination must receive the local certificate.

Conference settings

Field	Field description	Usage tips
Voice switching sensitivity	Determines how easy it is for a participant to replace the active speaker for a conference based on how loudly they are speaking.	A value of 0 means that it is very difficult for the active speaker to be replaced; a value of 100 means the active speaker can be replaced very easily.
Packet loss threshold	Enter the threshold level for packet loss as a percentage. If greater packet loss occurs than this threshold, it will be reported: ■ in the Status page for the conference ■ in the Statistics page for the endpoint whose call is experiencing the packet loss	The most suitable setting will depend on your network and its packet loss characteristics.
ClearVision	When selected, the TelePresence Server will upscale video streams from participants who are sending low resolution video with the purpose of making best use of the TelePresence Server's HD video capabilities.	The TelePresence Server uses intelligent resolution upscaling technology to improve the clarity of low-resolution video.
Enable 60 fps	Allows the TelePresence Server to support 60 frames per second video streams.	*HD* mode supports 60 fps at a maximum resolution of w448p. *Full HD* mode supports 60 fps at a maximum resolution of 720p. Lower resolution streams may also have 60 fps.

Field	Field description	Usage tips
HD mode	Defines the maximum video definition that the TelePresence Server will support. One of *HD* or *Full HD*. If you change this setting, your change will take effect as soon as there are no participants connected to the TelePresence Server.	*HD* mode supports a maximum definition of 720p at 30fps, or w448p at 60 fps. *Full HD* mode supports a maximum definition of 1080p at 30 fps, or 720p at 60 fps. An endpoint that uses *Full HD* mode consumes more of the TelePresence Server resources than one using *HD* mode. This affects the maximum number of Full HD participants; see ports allocation for more details.
Call out using conference name	Allows the TelePresence Server to display the conference name to identify itself when calling out to participants.	Disabled by default. May not be displayed by all endpoints.
Call out to grouped endpoints if one calls in	If this option is selected, if a call is received from an endpoint which forms part of a manually-configured group the TelePresence Server will call out to the other endpoints in that group.	You should make sure this option is unchecked if the endpoints which make up manually-configured groups are set to call in together - in this case the TelePresence Server will recognise the separate calls and group them automatically.
Automatic content handover	Whether a participant is allowed to interrupt another participant's presentation in a conference by starting one of their own. This is unselected by default.	When selected, if an endpoint attempts to send content when another participant is already sending content, the endpoint would override or cancel any existing presentation.
Indicate presence of audio-only participants	Whether an overlaid icon is shown on video participants' screens to show the presence of audio-only participants in the conference. This is unselected by default.	When selected, a telephone icon is displayed in the top left-hand corner of the screen with a number next to it showing the number of audio-only participants present. For grouped endpoints, the icon is shown on just one of the screens: ■ the middle screen on T3s and Experias ■ for manually-configured groups, on the screen configured as the **Screen to receive content / audio** in the group's Advanced settings.
Display video preview images	When selected, thumbnail preview images of conference participants' video streams are shown on the TelePresence Server user interface.	

Default conference settings

Field	Field description	Usage tips
Show lobby screen	Enable the TelePresence Server to display lobby screens to participants. Participants see this screen when they join a conference or when there is no video to display (all other participants are either audio-only or have video muted, and self-view is disabled.)	The lobby screen shows the conference title, start and end times (if applicable), and an optional lobby message. The message is set on a per conference basis.
Lobby screen date format	Select one of the date/time formats to display start and end times on the lobby screen.	Conference start and end times only display for scheduled conferences that you create via the TelePresence Server's web interface.
Conference ending notification	Allows the TelePresence Server to warn participants that the conference is ending soon.	Participants will see a notification, two minutes prior to the end of the conference, that the conference is ending soon. Cisco CTS endpoints display an icon instead of a notification message. Other endpoints see the message overlaid on their displays. See the endpoint interoperability reference for details.
Use custom conference ending notification text	Allows the TelePresence Server to use a custom message to warn participants that the conference is ending.	The TelePresence Server uses a default message unless you enable and enter a custom message. The default message is `This conference is about to end`. Does not apply to Cisco CTS endpoints. See the endpoint interoperability reference for details.
Custom conference ending notification text	Enter a message that the TelePresence Server will use instead of the default message.	

Default endpoint settings

Field	Field description	Usage tips
Full screen view of single-screen endpoints	This option sets the conditions under which single-screen endpoints are placed in full screen panes of video displays sent to conference participants.	This setting can be overridden by the equivalent Full screen view setting in single-screen endpoints' Configuration page. Select a setting from the drop-down list to be used as the default: ■ *Allowed*: Single-screen endpoints will always be allowed to be shown in full screen panes. ■ *Dynamic*: Single-screen endpoints will be allowed to be shown in full screen panes if there are no grouped endpoints to show. However, when there are grouped endpoints to show, single-screen endpoints will then be restricted to the smaller continuous presence panes. ■ *Disabled*: Single-screen endpoints will never be shown in full screen panes.
Show borders around endpoints	Select this option to show borders around participants displayed in the conference view sent to new endpoints/endpoint groups by default.	For more information, see Understanding how participants display in layout views. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Active speaker display	Select this option to show a red border around the active speaker.	This setting is only available if *Show borders around endpoints* (detailed above) is selected.
Show endpoint names as panel labels	If you select this option, the TelePresence Server will label view panes in the conference layout sent to new endpoints/endpoint groups by default with the names of the participants shown in those panes.	This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Show continuous presence panes	Select this option to allow a mixture of small and large panes in the view sent to new endpoints by default so that additional participants can be displayed.	For more information, see Understanding how participants display in layout views. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Self view	If you unselect this option, the TelePresence Server will never show the video stream sent from this endpoint or endpoint group to the participants using this endpoint or endpoint group by default i.e. they will not see themselves.	For more information, see Understanding how participants display in layout views. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.

Field	Field description	Usage tips
Use panel switched view as default	This option controls the default layout single-screen endpoints see when they connect. Participants can change their layout using Far End Camera Control. When selected, any single-screen endpoint will use the panel switched view upon connection. In this 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.	When using the panel switched view, the loudest panel/screen of a multi-screen endpoint is displayed full-screen to single-screen endpoints. The panel switched view requires that the multi-screen systems in the conference send the TelePresence Server a loudest panel/screen indication. If multi-screen systems that do not provide this indication are participating in a conference, only the standard single-screen continuous presence view of these endpoints are available. See the endpoint interoperability reference for a list of the multi-screen systems that reveal the loudest panel information.
Allow content in main video	This feature allows the TelePresence Server to send a conference's content channel in the main video channel of endpoints that don't support the extra channel. Endpoints that would otherwise be unable to see the content channel can see it if you enable this feature. In these cases, the content channel video is shown in the largest pane of a composed layout. The content layout replaces the main video while the content channel is active (audio is unaffected).	When content is shown in main video it does not consume a content port. The TelePresence Server can dynamically apply this feature, if there is competition for content ports, to maximize the chance of all participants seeing the content. Content does not entirely replace the main video; the content displays in the largest pane of a composed layout that also shows the other participants' streams across the bottom of the screen (more about layouts). This setting can be overridden by the equivalent field in the endpoint's or endpoint group's Configuration page. For more information about the content channel, see Content channel video support.

Field	Field description	Usage tips
Video format	The format to be transmitted by the TelePresence Server to an endpoint or endpoint group.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. NTSC is typically used in North America, while PAL is typically used in the UK and Europe. Select a setting from the drop-down list: ■ *PAL - 25fps*: The TelePresence Server will transmit video at 25 frames per second (or a fraction or multiple of 25, for example: 50 or 12.5fps) ■ *NTSC - 30 fps*: The TelePresence Server will transmit video at 30 frames per second (or a multiple or fraction of 30, for example: 60 or 15fps)
Transmitted video resolutions	The setting for transmitted video resolutions from the TelePresence Server to an endpoint or endpoint group.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. Select a setting from the drop-down list to be used as the default : ■ *4:3 resolutions only* ■ *16:9 resolutions only* ■ *Allow all resolutions* (4:3 and 16:9 are the preferred options - avoid using *Allow all resolutions* if possible)
Motion/sharpness tradeoff	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between an endpoint or endpoint group and the TelePresence Server. This setting controls how the TelePresence Server will negotiate the settings to be used.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. Select a setting from the drop-down list to be used as the default: ■ *Favor motion*: the TelePresence Server will try and use a high frame rate. That is, the TelePresence Server will strongly favor a resolution of at least 25 frames per second ■ *Balanced*: the TelePresence Server will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second) ■ *Favor sharpness*: the TelePresence Server will use the highest resolution that is appropriate for what is being viewed

Field	Field description	Usage tips
Default bandwidth (both to and from the server)	The network capacity used by the media channels established by the TelePresence Server to unknown endpoints and to new pre-configured endpoints for which a value has not been set.	When the TelePresence Server makes a call to an endpoint, it chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio, video, and content channels combined. For endpoint groups, this is the maximum bandwidth per endpoint. This setting can be overridden for individual endpoints in the Advanced settings page.
Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the TelePresence Server for outgoing video streams (from the TelePresence Server to connected endpoints and endpoint groups).	This setting can be overridden for individual endpoints in the Advanced settings page. Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The Cisco TelePresence Server optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size. Increasing this value can cause fragmentation of packets which impairs performance and can cause packet loss. Decreasing this value too much can also impair performance. **Note:** You should only modify this setting if there is a known packet size restriction in the path between the Cisco TelePresence Server and potential connected endpoints.

Field	Field description	Usage tips
Received video: flow control on video errors	Selecting this check box allows the TelePresence Server to request that the endpoint or endpoint group send lower speed video if it fails to receive all the packets which comprise the far end's video stream.	The TelePresence Server can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased based on the quality of video received by the TelePresence Server. If there is a bandwidth limitation in the path between the endpoint/endpoint group and the TelePresence Server, it is better for the TelePresence Server to receive every packet of a lower rate stream than to miss some packets of a higher rate stream. This setting can be overridden by the **Received video: flow control on video errors** field in an endpoint's or endpoint group's Advanced configuration page.
Received video: flow control based on viewed size	Selecting this check box allows the TelePresence Server to request that the endpoint or endpoint group send lower speed video if the use of the video from that endpoint does not require as high a speed as the channel allows.	Typically the TelePresence Server would send a flow control message because of this setting if the video from that endpoint was either not being seen at all by other conference participants or if it was being shown only in small layout panes. This setting can be overridden by the **Received video: flow control based on viewed size** field in an endpoint's or endpoint group's Advanced configuration page.
Video transmit size optimization	Allows the TelePresence Server to vary the resolution, or resolution and codec, of the video being sent to a remote endpoint within the video channel established to that endpoint. Select a setting from the drop-down list: ■ *None*: Do not allow video to be optimized during transmission ■ *Dynamic resolution only*: Allow video size to be optimized during transmission ■ *Dynamic codec and resolution*: Allow video size and codec to be changed during transmission	With this option enabled, the TelePresence Server can, for instance, decide to send CIF video within a 4CIF channel if this will increase the viewed video quality. The circumstances under which decreasing the video resolution can improve the video quality include: ■ if the original size of the viewed video is smaller than the outgoing channel ■ if the remote endpoint has used flow control commands to reduce the bandwidth of the TelePresence Server video transmission Typically, lowering the resolution means that the TelePresence Server can transmit video at a higher frame-rate. This setting can be overridden by the **Video transmit size optimization** field in an endpoint's or endpoint group's Advanced configuration page.

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.

Upgrading and backing up 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. Shutting down and restarting the TelePresence Server.

Upgrading the loader software image

Upgrades for the loader software image are not typically 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. Shutting down and restarting the TelePresence Server.

Backing up and restoring the configuration

The Back up and restore section of the **Upgrade** (**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 the button 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 select **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 were restoring from a file backed up from the same TelePresence Server or if you were 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 boxes may become unreachable via IP. If you do not select **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 select the **User settings** check box, 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.
  Configured rooms are linked to user accounts and therefore the **User settings** overwrite control also controls whether configured rooms are overwritten by the contents of the uploaded file — configured rooms will be left unaltered if the **User settings** check box is not selected.

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's 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.

Upgrade 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 the button 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.

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

To shut down the TelePresence Server:

1. Go to **Configuration > Shutdown**.
2. Click the **Shut down TelePresence Server** button.
   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 password

This page allows you to change the administrator password used to log in to this TelePresence Server. 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**.

(A room's password is changed in its configuration page.)

Back up and restore 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 Numeric ID instead, click the relevant column heading.

On this page you can:

- Add or delete pre-configured conferences. You cannot delete conferences that were started from rooms; the TelePresence Server automatically deletes them when appropriate.
- Click a conference name to display its status:
  - for a pre-configured conference, you can also edit its configuration.
  - for a conference started from a room, you'll see the room's status page instead.
- Click the cog icon next to a conference name to display its configuration.

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 or the name of the room where the conference was created.	Click the conference name to display conference status and participants. The name of a conference started from a room has the word *(room)* after the room's name.
Numeric ID	The numeric ID assigned to the conference.	This is the ID that the TelePresence Server uses to register the conference with a gatekeeper or registrar. The TelePresence Server will not attempt to register the ID with the gatekeeper unless the **Use gatekeeper** option is selected. It will not try to register with a SIP registrar unless **Outbound call configuration** is set to *Use registrar*. Both settings are on the **Configuration > System settings** page.

Field	Field description	Usage tips
Status	The status of the conference: ■ *Scheduled* ■ *Enabled* ■ *Active* ■ *Inactive* ■ *Completed*	Conferences can be: ■ A *Scheduled* conference shows the scheduled start and end times. ■ An *Enabled* conference has no start or end time but it does have a numeric ID. An endpoint user can call the TelePresence Server with this numeric ID to start the conference. Its status will change to *Active (<X> endpoints)* while there are active participants. ■ An *Active* conference may also display the number of participants and the scheduled end time. ■ An *Active* conference may also be *permanent* and may not currently have active participants (a permanent conference has no configured end time). ■ An *Inactive* conference has no start or end time and does not have a numeric ID. You can only start the conference from its **Status** or **Configuration** page. ■ A *Completed* conference had a scheduled end time which has passed. The status may have additional information about the conference duration, and whether it is locked and for how long. For example, *Inactive - Due to end in 5 hours and 27 minutes [Locked - will be unlocked in 2 hours and 7 minutes]*.

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 registered to an H.323 gatekeeper or SIP registrar
- is locked
- has port limits, and what they are
- includes a content channel
- has participants and the status of each
- had previous participants and who they were

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

- Click **Call endpoint** to invite participants to join this conference
- Click an endpoint name to see the endpoint's status

For active conferences you can also:

- 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* ■ *Enabled* ■ *Active* ■ *Inactive* ■ *Completed*	Conferences can be: ■ *Active (<X> endpoints) - due to end <time>*: this conference is in progress and has a scheduled end time. ■ *Active - permanent*: this is a permanent conference which has past its start time but may or may not have any active participants. ■ *Inactive*: this conference does not have a scheduled start or end time, nor a numeric ID. It can only be started from the conference's status or configuration pages. ■ *Enabled*: this conference does not have a scheduled start or end time but has a numeric ID, therefore an endpoint can call to the TelePresence Server with this numeric ID and start the conference. It will then be shown as *Active (<X> endpoints)* while there are active participants. ■ *Completed*: this conference had a scheduled end time which has passed. The status may have additional information about the conference duration, and whether it is locked and for how long. For example, *Inactive - Due to end in 5 hours and 27 minutes [Locked - will be unlocked in 2 hours and 7 minutes]*.
H.323 gatekeeper status	The status of a conference with respect to its H.323 gatekeeper.	One of: ■ *Numeric ID registered* ■ *Numeric ID failed to register* ■ *Not registered:* conference is not configured to register with the gatekeeper ■ *Registering*: conference is in the process of registering If the TelePresence Server can connect to an H.323 gatekeeper, the name and numeric ID of a conference can be registered with that gatekeeper as a different directory number. This allows H.323 users to dial directly into a particular conference. To configure a H.323 gatekeeper, go to **Configuration > System settings**.

Field	Field description	Usage tips
SIP registrar status	The status of a conference with respect to its SIP registrar.	One of: ■ *Numeric ID registered* ■ *Numeric ID failed to register* ■ *Numeric ID unable to register (registration settings not configured)* conference is configured to try and register but it cannot because the system's SIP call configuration is set to *Use trunk* or *Call direct* instead of *Use registrar* ■ *Not registered:* conference is not configured to register with the registrar ■ *Registering*: conference is in the process of registering If the TelePresence Server can connect to a SIP registrar, the name and numeric ID of a conference can be registered with that registrar as a different directory number. This allows users to dial directly into a particular conference. To configure a SIP registrar , go to **Configuration > System settings**.
Conference lock status	Indicates whether the conference is locked.	
Port limits	Indicates whether the conference has port limits, and what those limits are.	
Content	Whether the content channel is currently in use.	One of: ■ *Disabled*: content sharing is disabled for the conference. To enable content for this conference, go to **Conferences > *conference name* > Configuration** ■ *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.
Enter/Leave OneTable mode	Allows you to force the conference's layout into or out of OneTable mode.	This button is only displayed if **Use OneTable mode when appropriate** is disabled for the conference in its **Configuration** page and if there are three or four participants in the conference using multi-screen endpoints. Not all multi-screen endpoints support OneTable mode. See the endpoint interoperability reference for a list of supporting endpoints.

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: ■ *No endpoints* - the conference has no active participants ■ *Not in a conference* - the endpoint is not active ■ *In conference* - the endpoint is currently participating in this conference. Additional status information may be displayed, for example, *audio muted*. If a pre-configured endpoint is busy when the conference starts, the TelePresence Server will retry the endpoint repeatedly throughout the conference and connect it if it becomes free.
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 endpoint may have disconnected for one of the following reasons: ■ *unspecified error*: the endpoint has disconnected, but the TelePresence Server does not know the reason ■ *no answer*: the endpoint has failed to connect because it did not answer ■ *call rejected*: the endpoint has failed to connect because it rejected the call ■ *busy*: the endpoint has failed to connect because it was busy ■ *gatekeeper error*: the endpoint has failed to connect because of a gatekeeper error ■ *left conference*: the endpoint has left the conference ■ *destination unreachable*: the endpoint has failed to connect because it was unreachable The TelePresence Server may have disconnected the endpoint for one of the following reasons: ■ *requested by administrator*: the endpoint has been disconnected by an administrator ■ *requested via API*: the endpoint has been disconnected via the API ■ *end of conference*: the endpoint has been disconnected at the end of a conference ■ *requested via web interface*: the endpoint has been disconnected via the web interface ■ *encryption unsupported*: the endpoint has been disconnected because it does not support encryption ■ *deleted*: the endpoint has been disconnected because the endpoint was deleted ■ *conference deleted*: the endpoint has been disconnected because the conference was deleted ■ *group disconnect*: the endpoint has been disconnected because a group member disconnected ■ *TIP failed*: the endpoint has been disconnected because TIP negotiation failed ■ *no free resources*: the endpoint has been disconnected because there are no free resources ■ *configuration change*: the endpoint has been disconnected because of a configuration change ■ *disconnect timeout*: the endpoint has been

Field	Field description	Usage tips
		disconnected (timeout) ■ *TS deleted*: the endpoint has been disconnected because the hosting TelePresence Server has been deleted ■ *moved conference*: the TelePresence Server has disconnected the endpoint to move it to another conference

Adding and updating conferences

There are a number of ways to start a conference with the TelePresence Server:

- Using the TelePresence Server's web interface, as described in this topic.
- Logging in to the TelePresence Server from a room. See Logging in from a room.
- Calling directly into a conference from an endpoint. This is only possible if the conference has a numeric ID. If the numeric ID is registered with the gatekeeper/SIP registrar, you can dial the numeric ID on its own; if not, you can dial by TelePresence Server IP address plus numeric ID.

Adding a conference

To add a conference:

1. Go to **Conferences > Add new conference**.
2. Complete the fields, referring to the table below for more information.
3. Click **Add new conference**.

Notes:

- You can add pre-configured endpoints to a conference to be automatically invited into the conference by the TelePresence Server. This is useful if you regularly invite the same participants into a conference This is done on the conference configuration page after the conference has been created - see Updating a conference for more information.
- If a pre-configured endpoint is busy when the conference starts, the TelePresence Server will retry the endpoint ten times and connect it if it becomes available.
- You can schedule the conference timing, or return to the conference configuration subsequently and start the conference as an ad hoc conference using **Start now**.

Updating a conference

When updating a conference's configuration you can select endpoints to dial and then dial out and start an ad hoc conference using an existing conference configuration.

To update an existing conference:

1. Go to **Conferences**.
2. Click a Conference name. That conference's status page is shown.
3. Go to **Configuration**.
4. Edit the fields referring to the table below.
5. If required, add pre-configured endpoints to the conference configuration:
   i. Click **Add pre-configured participants**.
   ii. Select from the full list of pre-configured participants.

   Note: If you have scheduled a time for the conference, then you cannot select any endpoints or endpoint groups that are already configured for a conference during that period. This avoids clashing commitments for endpoints and endpoint groups.

   iii. Click **Update**.
   The participants are displayed in the **Pre-configured participant** section.
6. Click **Update conference**.

Starting an ad hoc conference with pre-configured participants

An ad hoc conference is one that is started from the web interface with the **Start now** button. This can be:

- based on a conference that was configured without a schedule.
- an additional ad hoc instance of a scheduled conference: in this case, the conference continues to its scheduled end time, if there is one, unless you disconnect the participants manually.

1. Go to **Conferences**.
2. Click the name of the conference whose configuration you want to use for this conference.
3. Go to **Configuration**.
4. If required, select pre-configured endpoints:
   i. Click **Add pre-configured participants**.
   ii. Selected the endpoints to be dialed and click **Update**.
5. Click **Start now** to start the conference immediately.

Conference configuration reference

Conference

Field	Field description	Usage tips
Name	The name of the conference.	Conference names do not need to be unique.
Numeric ID	The unique identifier used for dialing in to the conference.	Participants can only join a conference by dialing its numeric ID if the conference's numeric ID is registered with the H.323 gatekeeper or SIP registrar (depending on which protocol the endpoint is using). If the conference has a numeric ID that is not registered, you can join the conference by dialing the IP address of the TelePresence Server that is running the conference plus the numeric ID. Conferences do not have to have a numeric ID, but numeric IDs must be unique.
Register numeric ID with H.323 gatekeeper	Whether to register the conference with the Numeric ID as the H.323 ID.	Select this check box to register the conference's numeric ID with the gatekeeper (if H.323 registration is enabled on the **System Settings** page).
Register numeric ID with SIP registrar	Whether to register the conference's Numeric ID with the SIP registrar.	Select this check box to register the conference's numeric ID with the registrar (if SIP registration is enabled on the **System Settings** page)

Field	Field description	Usage tips
Conference locked	Locks a conference.	Check the box to lock the conference. You can still add pre-configured participants before the conference starts, but no participants will be able to join (call in) when the conference is active. You can call out to invite participants in to a locked conference.
Encryption	Whether encryption is optional or required for this conference.	If encryption is *Required*, only endpoints that support encryption can join this conference. Encryption requires a feature key. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server.
Use OneTable mode when appropriate	Whether to use OneTable mode automatically when the correct combination of endpoints or endpoint groups is in a conference (three or four telepresence endpoints plus less than six other endpoints or endpoint groups). Choose from: ■ *Disabled* ■ *2 person mode* ■ *4 person mode*	In OneTable mode each screen shows an entire view of a single remote site (as opposed to one third of the remote site in a normal, point-to-point telepresence setting). This allows the center four or two participants in three remote telepresence rooms to be seen simultaneously, as if they were seated at one table - depending on whether *4 person mode* or *2 person mode* is selected. For more information, see Understanding how participants display in layout views. Not all multi-screen endpoints support OneTable mode. See the endpoint interoperability reference for a list of supporting endpoints.
Content channel	If *Enabled*, this conference is able to support an additional video stream, sent potentially to all connected endpoints, intended for showing content video. This content video is typically high resolution, low frame rate data such as a presentation formed of a set of slides. Such presentation data can be sourced by an endpoint specifically contributing a separate content video stream.	For more information, see Content channel video support.

Port limits and lobby settings

Field	Field description	Usage tips
Video	Enable a limit on the video ports allowed for this conference	Check the box and enter the maximum number of video ports you want this conference to use. The TelePresence Server can not guarantee to provide this number of ports. However, if more than this number are requested and available, the TelePresence Server will supply ports until the limit is reached.
Audio only	Enable a limit on the number of audio only ports allowed for this conference	Check the box and enter the maximum number of audio only ports you want this conference to use. The TelePresence Server can not guarantee to provide this number of ports. However, if more than this number are requested and available, the TelePresence Server will supply ports until the limit is reached.
Show lobby screen	Enable a lobby screen for this conference.	The lobby screen can be enabled/disabled on a server-wide basis. If you select <*Use default*> here, the conference will inherit the setting from the **Configuration > System settings** page. Otherwise, you can select *Enable* or *Disable* to override the server-wide setting.
Lobby message	Display a custom message on the lobby screen.	Enter some text to display on the lobby screen. If **Show lobby screen** is enabled—either because it is enabled by the server-wide setting or enabled for this conference only—participants will see this text when they see the lobby screen.

Scheduling

Field	Field description	Usage tips
Schedule	Select the check box to enable the settings in this section.	Conferences can be scheduled using the fields in this section, but you may also want to create a conference without a set start time (in this case, leave this setting unselected). Subsequently, when you want the conference to start, open the conference configuration, add endpoints and click **Start now**.
Start time	The date and time at which the conference will begin.	By default the current date and time are displayed.

Field	Field description	Usage tips
Permanent	Allows you to retain a conference and its settings for an infinite period of time.	
End time	The date and time at which the conference will finish.	These fields are not available or necessary for permanent conferences.
Conference ending notification	Send a message to all participants when the conference is coming to an end.	This notification can be enabled/disabled on a server-wide basis. If you select <*Use default*> here, the conference will inherit the setting from the **Configuration > System settings** page. Otherwise, you can select *Enable* or *Disable* to override the server-wide setting. You can edit the message on a server-wide basis on the **System settings** page.

Call endpoints to join a conference

1. Go to the **Conference > Conference name > Status** page.
2. Click **Call endpoint** if you want to invite one or more participants to join.
3. The **Call endpoint** page displays.
   Here you can call endpoints that the TelePresence Server knows about as well as those that it doesn't know about.

Call known endpoints

The **Endpoints** list contains all the endpoints that are known to the TelePresence Server. This list may span more than one page, in which case there are links to all the pages near the bottom of each page.

1. Select the endpoints you want to call by checking the boxes next to the endpoint names.
   You can select all or clear all by checking the box in the heading row.
2. Click **Call selected**.

Call an unknown endpoint

If an endpoint you want to invite is not in the **Endpoints** list:

1. Enter its IP address, URI, or E.164 number in the **Address** field.
2. Select the **Call protocol** to use.
3. Check **Call direct** if necessary.
   You'll have to enter the full IP address if you check this option. You should only need to do this if the endpoint is not registered with either the gatekeeper or registrar.
4. Select the **Bandwidth** you want to allow for this call, from 64 kbps up to 6 Mbps.
5. Enter a **Send DTMF** sequence if necessary.
   This is usually unnecessary. However, a DTMF sequence may be required by the endpoint, for example a numeric PIN, in which case enter the keypress sequence here.

Send a message to participants

You can send a message to all endpoints in an active conference or to just one of the endpoints. The instructions are the same but you'll access different pages to send the message:

- To send a message to one participant: Go to **Endpoints > *Endpoint Name* > Status** and click **Send message**. You could also click the endpoint name in the conference's status page to get to the endpoint's status page.
- To send a message to all participants: Go to **Conferences > *Conference Name* > Status** and click **Send message**.

The **Send message** page displays.

Note: Very long messages might not display properly on some screens so you should consider limiting your messages to a maximum of a few hundred characters.

On the **Send message** page:

1. Type your message in the **Message** field.
2. Click one of the nine radio buttons (the three by three grid labeled **Position**) to select where the message will display on the target system(s).
3. Enter a **Duration** (in seconds) for the message to stay on the endpoint screen(s).
4. Click **Send message**.
   The TelePresence Server displays your message on the screen(s) of the endpoint(s).

Endpoints and endpoint groups

Endpoints

The **Endpoints** page is where you can see or edit endpoints and add new ones. The term endpoints refers to the logical ends of a video conference and includes single- or multi-screen systems, immersive telepresence systems, Cisco CTS systems, endpoint groups and devices like the Cisco TelePresence IP VCR.

An endpoint group is a set of two or more endpoints that has one name and can be selected as the recipient of a call. The component endpoints are treated as one endpoint by the TelePresence Server.

Note: Multi-screen endpoints are not the same as endpoint groups.

The list of endpoints contains pre-configured and active endpoints and endpoint groups. You can use this list as a starting point to view or edit a specific endpoint.

When you pre-configure endpoints it is easier to add them to conferences; you can choose names from a list rather than manually entering names or addresses.

Recordings as endpoints

If you configure the IP VCR as an endpoint, then add it as a participant in a conference, it will start recording when the conference starts. You can also configure a folder's Recording ID as an endpoint, in which case the IP VCR records directly to the specific folder.

Also, if you configure a specific recording as an endpoint, a participant can contribute the recording as a video stream. This feature is useful if you want to view a recording within a conference.

For more information refer to the IP VCR documentation.

The list of endpoints

Go to **Endpoints** to display the list of endpoints.

The interface displays the list in alphabetical order by default. Click on a column heading to order by that column instead.

On this page you can:

- See an endpoint's status or edit its settings; click on the endpoint name
- Add an endpoint; click **Add new endpoint**
- Add a legacy Cisco CTS endpoint; click **Add legacy Cisco CTS endpoint**
- Add an endpoint group (if activated); click **Add grouped endpoints**
  A feature key is required to activate the endpoint groups feature. The button only displays if the key is installed.
- Delete preconfigured endpoints; select the endpoints and click **Delete selected**.

Each item in the list has the following information:

Endpoint list details

Field	Field description
Name	The name of the endpoint.
Type	The type of endpoint, for example: 'Cisco three screen telepresence', 'Standard', or 'Group of *N* endpoints' (see Endpoint types for more details).
Status	Whether the endpoint is in a conference and, if it is, the name of the conference.

Display endpoint and group status

The endpoint status is most useful when the endpoint is part of an active conference. You can also control the endpoint to some extent from here.

1. Go to **Endpoints**
2. Click on an endpoint or group name
3. Review or control the endpoint, with reference to the following table
4. Refresh the page in your browser to get the latest status.

Endpoint-supplied information

Field	Field description	Usage tips
Country code/extension	These fields display information as returned by the endpoint. The details may not be supplied in a consistent manner between manufacturers.	This information is displayed after the endpoint has been connected for the first time (regardless of whether it's currently connected or not).
Manufacturer code		
Product		
Version		

Status

Field	Field description	Usage tips
Connected to conference	Whether the endpoint is currently in a conference, and if so the name of the conference.	Click the conference name to go to the status page for that conference.
Call status	Whether the call is connected and if so, if it is an incoming or outgoing call.	
Protocol	The protocol used in this call e.g. H.323.	
Endpoint advertised capabilities	The capabilities that the endpoint advertised when negotiating the call.	For example: Audio, Video, Video content, Encrypted traffic, Unencrypted traffic.
Video channels	Whether receive and transmit video channels are open between the Cisco TelePresence Server and the far end.	
Far end audio mute	Whether the audio from the far end has been muted by the remote device.	
Bandwidth	The amount of network bandwidth used for this call's media in each direction.	For an endpoint group, this shows the bandwidth for each call rather than the total combined bandwidth.

Field	Field description	Usage tips
Encryption check code	If encryption is in use for this call, the encryption check code is shown here.	The check code can be used in combination with information displayed by some endpoints to check that the encryption is secure.
Preview	Sample stills of the video stream(s).	The preview shows a still from each screen for both the receive stream (top row) and the transmit stream (bottom row).
Endpoint *X*	(Endpoint groups only) The IP address and connection status of each endpoint in an endpoint group.	
Duration	The time that the endpoint/endpoint group has been in this conference.	
Disconnect	Use this control to disconnect the endpoint or endpoint group from the conference.	
Mute audio from / **Unmute audio from**	Use this control to start or stop muting audio from this endpoint. This changes whether other conference participants will be able to hear this endpoint.	
Mute audio to / **Unmute audio to**	Use this control to start or stop muting audio to this endpoint. If audio is muted *to* an endpoint, the endpoint will hear silence.	
Mute video from / **Unmute video from**	Use this control to start or stop muting video from this endpoint. This changes whether other conference participants will be able to see this endpoint.	
Mute video to / **Unmute video to**	Use this control to start or stop muting video to this endpoint. If video is muted *to* an endpoint, that endpoint will be sent blank video.	
Tidy view	Use this control to tidy the view layout being sent to this endpoint or endpoint group.	The TelePresence Server automatically centers the PIPs (pictures in picture) showing the video streams of other participants, and moves the PIPs between screens if doing so means it can display the PIPs slightly larger. This happens dynamically as participants join and leave the conference. Use the tidy view option if necessary to manually reset and center the participants' PIPs in the layout sent to this endpoint.

Field	Field description	Usage tips
Send message	Send a message to the endpoint.	When you click the button, the **Send message** page displays: 1. Enter your message, select its position on the target endpoint, and enter a duration (in seconds) for the message to display. 2. Click **Send message**.

Add an endpoint

1. Go to **Endpoints > Add new endpoint**.
2. Configure the endpoint with reference to the edit endpoint topic.

   Note: If you want to be able to call out to this endpoint from a conference, you must configure its **Call-out parameters**.

3. Click **Add new endpoint**.

Add a legacy Cisco CTS endpoint

This feature only applies to a specific class of endpoints running particular versions of their operating software. Refer to the endpoint interoperability reference for details.

1. Go to **Endpoints > Add legacy Cisco CTS endpoint**.
2. Enter the **Name** and **Address** of the endpoint.
   This is the call-out address; the TelePresence Server uses this to place outgoing calls to the endpoint. For example, this may be the SIP URI of the endpoint.
3. Click **Add legacy Cisco CTS endpoint**.
4. Configure the endpoint with reference to the settings in the edit endpoint topic.

   Note: If you want to be able to call out to this endpoint from a conference, you must configure its **Call-out parameters**.

5. Click **Update endpoint**.

Add an endpoint group

Note: A multi-screen endpoint is not the same as an endpoint group.

You can configure individual endpoints to work as a single, immersive endpoint. To use this feature you must have the "Third party interop" feature key installed. You can install feature keys on the **Configuration > Upgrade** page. (See Upgrading and backing up the Cisco TelePresence Server.)

To add an endpoint group:

1. Go to **Endpoints > Add grouped endpoints**.
2. Enter the **Name** of the group and the addresses of its members. See the first table below.
3. Click **Add grouped endpoints**.
4. Configure the endpoint group in the same way as you would configure an individual endpoint. Refer to the edit endpoint topic for details of the settings.

Endpoint group members

Endpoint group settings

Field	Field description	Usage tips
Name	The name of the group.	
Calling out address list	The list of addresses to call out to when this group is in an active conference.	Enter a list of addresses separated by commas. **Note:** The order must be from left to right in terms of facing the endpoints' screens.
Use gatekeeper	Select this check box to use a gatekeeper when calling this group.	This setting has no effect if the Cisco TelePresence Server is not configured to use a gatekeeper in the **Configuration > System settings** page.

Edit an endpoint's configuration

1. Go to **Endpoints**.
2. Click the name of the endpoint or group.
3. Go to **Configuration**.
4. Edit the configuration with reference to the following table.
5. Click **Update endpoint**.
6. You may also need to edit the advanced settings of the endpoint or group.

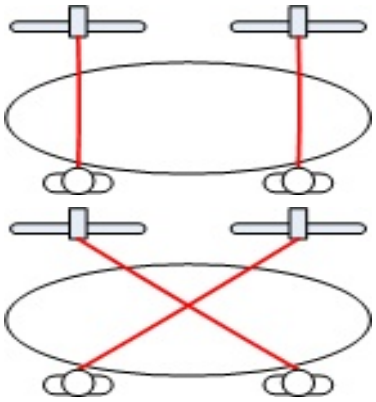
Endpoint settings reference

Note 1: Endpoints inherit the values for these settings from the **Default endpoint settings** section of the TelePresence Server's **System settings** page. If you change a local setting to something other than the inherited value, the endpoint's local setting always takes precedence over the system-wide setting.

Note 2: Not all of these settings apply to all endpoint types or groups. These differences are detailed in the table.

General settings

Field	Field description	Usage tips
Name	The name of the endpoint or endpoint group.	When you are updating an existing endpoint or endpoint group's configuration, its **Type** is also shown.
Type	The number of endpoints in the endpoint group is displayed.	Not applicable to individual endpoints.
Display name override	The name that will be displayed in a conference as a label for this endpoint or group.	The name you enter here will override any default name configured on the endpoint. It will also override any other default name that might appear for an endpoint. For example, an endpoint's default name can be the name of the gateway through which the call was placed, or if the endpoint is called-in via a gatekeeper, its E.164 number. **Note**: After an endpoint has connected, you cannot change the display name.
Minimum screen layout	When choosing which conference layout to send to a participant the Cisco TelePresence Server takes into account the number of screens used by other participants in the conference.	For more information, see Understanding how participants display in layout views.
Received audio gain	Adjusts the amplification of the incoming audio signal.	A fixed audio gain of between -12 dB and +12 dB (in 3 dB steps) is applied to an endpoint's incoming audio.
Transmitted audio gain	Adjusts the amplification of the outgoing audio signal.	A fixed audio gain of between -12 dB and +12 dB (in 3 dB steps) is applied to an endpoint's outgoing audio.

Field	Field description	Usage tips
Cameras are cross connected	Select this check box for endpoint groups whose outermost camera views cross. This option is only available for endpoint groups.	

Call-out parameters

Field	Field description	Usage tips
Address	The IP address, host name, E.164 address, or URI of the endpoint.	The TelePresence Server uses this information to contact the endpoint when it invites the endpoint to join a conference. For H.323 calls, you can configure this endpoint or endpoint group as needing to be reached via an H.323 gateway. To do this, set this field to be *<gateway address>!<E.164>*.
Call protocol	Select either H.323 or SIP from the drop-down list.	Not applicable to Cisco CTS endpoints which always use SIP.
Call direct	Select this option to allow the TelePresence Server to call this endpoint directly, via its IP address, instead of using the H.323 gatekeeper or SIP registrar (or trunk).	If the box is unchecked, which is the default setting, the TelePresence Server attempts to call the endpoint via a gatekeeper, registrar or trunk (depending on the server-wide system settings and the protocol the endpoint uses). This option does not apply to legacy Cisco CTS endpoints, which must be called via a registrar or trunk.
Send DTMF	Enter a string of DTMF characters if required.	If the endpoint needs a sequence of tones after connection, the TelePresence Server will send the tones matching the string you enter. The TelePresence Server supports the tones for the characters **`0-9`**, **`A-D`**, **`*`** and **`#`**. The TelePresence Server ignores invalid characters but continues sending tones for valid characters until it reaches the end of the string.

Call-in match parameters

Field	Field description	Usage tips
Name	The name that the endpoint or endpoint group sends to the Cisco TelePresence Server.	These fields are used to identify incoming calls as being from the endpoint or endpoint group. The endpoint or endpoint group is recognized if any of this information matches the identification sent by the endpoint. The TelePresence Server ignores empty fields when it is trying to match the endpoint. When you configure ***Call-in match parameters***, an endpoint or endpoint group will be recognized as this pre-configured endpoint or endpoint group and the ***Initial status*** parameters will be applied to a call from this endpoint or endpoint group. **Note:** For CTS systems, we recommend using the CTS directory number (DN) in the E.164 field.
Address	The IP address of the endpoint or endpoint group.	
E.164	For H.323 calls, the E.164 address with which the endpoint or endpoint group is registered with the gatekeeper. For SIP calls, the SIP username with which the endpoint or endpoint group is registered with the SIP registrar.	

Initial status

Field	Field description	Usage tips
Audio from	Whether the initial audio from the endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, it will not be able to contribute audio to the conference. For example, you can mute audio from an endpoint or endpoint group if somebody wants to be seen in the conference, but does not want to contribute verbally. You can mute both audio and video if required. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.
Audio to	Whether the initial audio to this endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, the participant using this endpoint or endpoint group will not be able to hear the other participants. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.
Video from	Whether the initial video from this endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, it will not be able to contribute video to the conference. For example, you can mute video from an endpoint or endpoint group if somebody wants to see the conference, but not be seen themselves. You can mute both audio and video if required. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.

Field	Field description	Usage tips
Video to	Whether the initial video to the endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, the participant using this endpoint or endpoint group will but not see the other participants, but will be seen themselves. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.

Display parameters

Field	Field description	Usage tips
Full screen view	This option controls the conditions under which this endpoint will be displayed full screen. This option is only available for single-screen endpoints and does not apply to Cisco endpoints or endpoint groups.	Select a setting from the drop-down list: ■ *Allowed*: This single-screen endpoint will always be allowed to be shown in full screen panes. ■ *Dynamic*: This single-screen endpoint will be allowed to be shown in full screen panes if there are no grouped endpoints to show. However, when there are grouped endpoints to show, the endpoint will then be restricted to the smaller continuous presence panes. ■ *Disabled*: This single-screen endpoint will never be shown in full screen panes.
Show borders around endpoints	Select this option to show borders around participants displayed in the conference view on this endpoint or endpoint group.	For more information, see Understanding how participants display in layout views.
Active speaker display	Select this option to show a red border around the active speaker on this endpoint or endpoint group.	This setting is only available if **Show borders around endpoints** is selected.
Show endpoint names as panel labels	If you select this option, the Cisco TelePresence Server will label view panes in the conference layout sent to this endpoint or endpoint group with the names of the participants shown in those panes.	
Show continuous presence panes	Select this option to allow a mixture of small and large panes in the view sent to this endpoint or endpoint group so that additional participants can be displayed.	For more information, see Understanding how participants display in layout views.
Self view	If this option is not selected, the Cisco TelePresence Server will never show the video stream sent from this endpoint or endpoint group to the participants using this endpoint or endpoint group i.e. they will not see themselves.	For more information, see Understanding how participants display in layout views.

Field	Field description	Usage tips
Use panel switched view as default	This option controls the default layout single-screen endpoints see when they connect. Participants can change their layout using Far End Camera Control. When selected, any single-screen endpoint will use the panel switched view upon connection. In this 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.	When using the panel switched view, the loudest panel/screen of a multi-screen endpoint is displayed full-screen to single-screen endpoints. The panel switched view requires that the multi-screen systems in the conference send the TelePresence Server a loudest panel/screen indication. If multi-screen systems that do not provide this indication are participating in a conference, only the standard single-screen continuous presence view of these endpoints are available. See the endpoint interoperability reference for a list of the multi-screen systems that reveal the loudest panel information.

Content parameters

Field	Field description	Usage tips
Video contribution	Whether this endpoint or endpoint group is permitted to contribute content to the conference via content channel.	To use the content channel, the content channel must be enabled for the conference in its configuration page.
Allow content in main video	Whether the Cisco TelePresence Server should send content channel video to this endpoint in its main video channel if it is not able to receive a separate video channel. This option is only available for single-screen endpoints and single-screen Cisco endpoints.	This option can be configured to match the Cisco TelePresence Server system settings (**Configuration > System settings**) or to be specifically *Enabled* or *Disabled* just for this endpoint.

Configure advanced settings of endpoints and groups

1. Go to **Endpoints**
2. Click the endpoint or group name
3. Go to **Advanced settings**
4. Configure the advanced settings with reference to the following table
5. Click **Update endpoint**.

Video settings

Field	Field description	Usage tips
Video format	The format to be transmitted by the TelePresence Server to an endpoint or endpoint group.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. NTSC is typically used in North America, while PAL is typically used in the UK and Europe. Select a setting from the drop-down list: ■ *PAL - 25fps*: The TelePresence Server will transmit video at 25 frames per second (or a fraction or multiple of 25, for example: 50 or 12.5fps) ■ *NTSC - 30 fps*: The TelePresence Server will transmit video at 30 frames per second (or a multiple or fraction of 30, for example: 60 or 15fps)
Transmitted video resolutions	The setting for transmitted video resolutions from the Cisco TelePresence Server to this endpoint or endpoint group.	Select a setting from the drop-down list: ■ *4:3 resolutions only* ■ *16:9 resolutions only* ■ *Allow all resolutions* Endpoints advertise the resolutions that they are able to display. The Cisco TelePresence Server then chooses the resolution that it will use to transmit video from those advertised resolutions. However, some endpoints do not display widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the Cisco TelePresence Server for transmissions to this endpoint or endpoint group.
Motion / sharpness trade off	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint or endpoint group and the Cisco TelePresence Server. This setting controls how the Cisco TelePresence Server will negotiate the settings to be used.	Select a setting from the drop-down list: ■ *Favor motion*: the Cisco TelePresence Server will try and use a high frame rate. That is, the Cisco TelePresence Server will strongly favor a resolution of at least 25 frames per second ■ *Favor sharpness*: the Cisco TelePresence Server will use the highest resolution that is appropriate for what is being viewed ■ *Balanced*: the Cisco TelePresence Server will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)

Network settings

Field	Field description	Usage tips
Default bandwidth (both to and from the endpoint)	The network capacity used by the media channels established by the Cisco TelePresence Server to and from this endpoint or endpoint group.	When the Cisco TelePresence Server makes a call to an endpoint, it chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio, video, and content channels combined. This setting overwrites (for this endpoint) the **Default bandwidth (both to and from the server)** setting made for all endpoints on the **Configuration > System settings** page.
Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the Cisco TelePresence Server for outgoing video streams (from the Cisco TelePresence Server to connected video endpoints).	Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The Cisco TelePresence Server optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size. Increasing this value can cause fragmentation of packets which impairs performance and can cause packet loss. Decreasing this value too much can also impair performance. **Note:** You should only modify this setting if there is a known packet size restriction in the path between the Cisco TelePresence Server and potential connected endpoints.

Optimization settings

Field	Field description	Usage tips
<use default>	Selecting this check box overrides any settings in the next three fields and uses the equivalent default conference settings.	The default conference settings are on the **Configuration > System settings** page.
Received video: flow control on video errors	Selecting this check box allows the Cisco TelePresence Server to request that the endpoint/endpoint group send lower speed video if it fails to receive all the packets which comprise the far end's video stream.	The Cisco TelePresence Server can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased based on the quality of video received by the Cisco TelePresence Server. If there is a bandwidth limitation in the path between the endpoint/endpoint group and the Cisco TelePresence Server, it is better for the Cisco TelePresence Server to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.

Field	Field description	Usage tips
Received video: flow control based on viewed size	If enabled, the Cisco TelePresence Server to requests that the endpoint or endpoint group send lower speed video if the use of the video from that endpoint does not require as high a speed as the channel allows.	Typically the Cisco TelePresence Server would send a flow control message because of this setting if the video from that endpoint was either not being seen at all by other conference participants or if it was being shown only in small layout panes.
Video transmit size optimization	Selecting this check box allows the Cisco TelePresence Server to vary the resolution, or resolution and codec, of the video being sent to a remote endpoint within the video channel established to that endpoint.	Select a setting from the drop-down list: ■ *None*: Do not allow video size to be changed during transmission ■ *Dynamic resolution only*: Allow video size to be optimized during transmission ■ *Dynamic codec and resolution*: Allow video size to be optimized during transmission and/or dynamic codec selection With this option enabled, the Cisco TelePresence Server can, for instance, decide to send CIF video within a 4CIF channel if this will increase the viewed video quality. The circumstances under which decreasing the video resolution can improve the video quality include: ■ if the original size of the viewed video is smaller than the outgoing channel ■ if the remote endpoint has used flow control commands to reduce the bandwidth of the Cisco TelePresence Server video transmission Typically, lowering the resolution means that the Cisco TelePresence Server can transmit video at a higher frame-rate.
Screen to receive content / audio	The address of the endpoint that audio and content channel video will be sent to when this endpoint group is in a conference. This option is only available for endpoint groups.	For more information about the content channel, see Content channel video support.

View endpoint or endpoint group statistics

1. Go to **Endpoints**.
2. Click on the endpoint or group name. The endpoint's **Status** page displays.
3. Go to **Statistics**.
   The information is displayed in up to four sections: **Audio**, **Auxiliary audio**, **Video**, and **Content channel**.
4. Refresh the page in your browser, or click **Refresh**, to get the latest statistics.

The statistics for each channel are grouped into two lists; **Receive stream** statistics and **Transmit stream** statistics.

Receive stream statistics

Field	Field description
Encryption	Whether this stream is encrypted.
Channel bit rate	The negotiated available bandwidth for the endpoint to send audio/video/content to the Cisco TelePresence Server.
Receive bit rate	This field applies to the Video and Content channel receive streams only. It is the bit rate (in bits per second) that the Cisco TelePresence Server has requested the endpoint sends. The most-recently measured bit rate displays in parentheses.
Received jitter	Represents the variation in timing between packets on this channel when they arrive at the Cisco TelePresence Server. Smaller numbers mean that the packets are arriving more predictably.
Receive energy	This field applies to the audio receive stream only and is a measure of the audio signal strength. The units are in millidecibels, with bigger negative numbers like -34000 being very quiet and negative numbers closer to zero being louder.
Packets received / errors	The number of audio packets that have been received by the Cisco TelePresence Server. The second number indicated the audio/video/content packet-level errors, for example, sequence discontinuities or incorrect RTP details. This is not the same as packets in which the video (the actual video data) is somehow in error.
Packets total / missing	The number of audio/video/content packets destined for the Cisco TelePresence Server from this endpoint. The second number indicates the number of packets that have been received but are corrupt.
Frames received / errors	The frame rate of the audio/video/content stream currently being sent to the endpoint and the number of frames with errors versus the total number of audio/video/content frames received.
Frame rate	This field applies to the video and content receive streams. It is the number of frames per second in the transmitted / received streams between the endpoint and the TelePresence Server.
Fast update requests sent	The number of fast update requests (FURs) sent by the TelePresence Server on this channel. For example, if packets are lost, the TelePresence Server sends a FUR to the endpoint.

Transmit stream statistics

Field	Field description
Encryption	Whether this stream is encrypted.
Channel bit rate	The negotiated available bandwidth for the Cisco TelePresence Server to send audio/video/content to the endpoint.
Transmit bit rate	This field applies to the video and content transmit streams only and is the bit rate the Cisco TelePresence Server is attempting to send at this moment. The actual bit rate, which is simply the measured rate of video data leaving the Cisco TelePresence Server, displays in parentheses.
Packets sent	The number of audio/video/content packets destined for the endpoint.
Frame rate	This field applies to video and content streams. It is the number of frames per second in the transmitted / received streams between the endpoint and the TelePresence Server.
Fast update requests received	The number of fast update requests (FURs) received by the TelePresence Server on this channel from the endpoint.

TelePresence Servers

Displaying the TelePresence Server list

Go to TelePresence Server to display all the TelePresence Servers that are configured to work with this Conference controller. This page may contain a maximum number of ten TelePresence Servers, and includes the controller itself.

For more information on the Conference controller, see Understanding the Conference controller.

Note: The Conference controlling arrangement is not the same as the clustering arrangement of multiple TelePresence Servers. For more information, see Comparing clustering with Conference controlling.

The TelePresence Servers are displayed in alphabetical order. Click on a column heading to order the list by that column.

On this page you can:

- Click a TelePresence Server's name to see its configuration and status.
- Click **Add new TelePresence Server** to enter the details of another controlled TelePresence Server.
- Select and then **Delete selected** TelePresence Servers. (You cannot delete the Conference controller).

TelePresence Server list details

Field	Field description
Name	The name of the TelePresence Server.
Address	The IP address of the TelePresence Server.
Software / build versions	The software and build versions running on the TelePresence Server.
Status	One of: ■ *Waiting for IP address* ■ *Connecting...* ■ *Connected: Waiting for final phase...* ■ *OK* ■ *Failed to connect to IP address <IP address>. Retrying in <X> seconds* ■ *Connection failed* ■ *Retrying dropped connection in <X> seconds* ■ *Disabled* ■ *Disabled - only conference controllers can manage other systems* ■ *There is a health status problem* ■ *Encryption not supported* ■ *Gatekeeper registration failed* ■ *Enhanced fonts not supported*
Screen licenses	The number of screen licenses associated with this TelePresence Server. For more information about licenses, see Understanding screen licenses.

Adding or updating controlled TelePresence Servers

Adding a controlled TelePresence Server to the Conference controller

Note: Before you can add the controlled TelePresence Server to the Conference controller, you must configure it to be managed by an external controller (see Understanding the Conference controller).

1. On the Conference controller, go to **TelePresence Servers > Add new TelePresence Server**.
2. Enter the details of the controlled TelePresence Server using the following table for reference.
3. Click **Add new TelePresence Server**.

Updating a TelePresence Server details on the Conference controller

1. On the Conference controller TelePresence Server go to **TelePresence Servers**.
2. Click on the name of the TelePresence Server you want to edit.
3. Edit the details of the controlled TelePresence Server using the following table for reference.
4. Click **Update TelePresence Server**.

The controlled TelePresence Server's status information is displayed below its configuration information.

TelePresence Server configuration reference

Field	Field description	Usage tips
Name	The name of the TelePresence Server.	
Address	The IP address of the TelePresence Server.	
HTTP port	The TCP port number on the TelePresence Server which the Conference controller TelePresence Server will attempt to connect to if it is configured to use HTTP for this connection.	This field is only displayed when you add a TelePresence Server.
HTTPS port	The TCP port number on the TelePresence Server which the Conference controller TelePresence Server will attempt to connect to if it is configured to use HTTPS for this connection.	This field is only displayed when you add a TelePresence Server.
Use HTTPS	When selected, this TelePresence Server will connect to the Conference controller TelePresence Server using HTTPS.	This field is only displayed when you add a TelePresence Server. If this option is selected, the TelePresence Server will use the **HTTPS port** value configured for the Conference controller TelePresence Server, otherwise it will use the **HTTP port** value.
Enabled	Whether this TelePresence Server is enabled.	If a TelePresence Server is not enabled, no conferences will be allocated to run on it by the Conference controller.

TelePresence Server status reference

Field	Field description	Usage tips
Connection status	Whether this TelePresence Server is connected to the Conference controller TelePresence Server.	One of: ■ *Waiting for IP address* ■ *Connecting...* ■ *Connected: Waiting for final phase...* ■ *OK* ■ *Failed to connect to IP address <IP address>. Retrying in <X> seconds* ■ *Connection failed* ■ *Retrying dropped connection in <X> seconds* ■ *Disabled* ■ *Disabled - only conference controllers can manage other systems* ■ *There is a health status problem* ■ *Encryption not supported* ■ *Gatekeeper registration failed*
Licenses	The number of screen licenses.	For more information about licenses, see Understanding screen licenses.
Model	The TelePresence Server model.	
Serial number	The unique serial number of the TelePresence Server.	
Software version	The installed software version. You will need to provide this information when speaking to customer support.	
Build	The build version of installed software. You will need to provide this information when speaking to customer support.	
Fans **Voltages** **RTC battery**	For enabled TelePresence Servers, shows Current status/Worst status seen conditions.	For each of current and worst seen conditions, one of ■ *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. This field is not displayed for *Disabled* TelePresence Servers.

Field	Field description	Usage tips
Temperature	For enabled TelePresence Servers, shows Current status/Worst status seen conditions.	Displays three possible states: ■ *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 the 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. This field is not displayed for disabled TelePresence Servers.
H.323 gatekeeper status	Whether the TelePresence Server is connected to an H.323 gatekeeper.	The gatekeeper's IP address is shown if the TelePresence Server is connected.
Number of active registrations	How many registrations the TelePresence Server has with the gatekeeper.	
SIP boxwide registration status	Whether the TelePresence Server is registered with a SIP registrar.	One of: ■ Registered <*server name*> with <*registrar address*> ■ Registration in progress ■ SIP registration not enabled ■ No registration configured ■ Failed to register <*server name*> to <*registrar address*>
Number of active conference registrations	How many conferences the TelePresence Server has registered with the gatekeeper.	
Features	What optional features are active on this slave TelePresence Server e.g. Encryption.	Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server.
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.

Field	Field description	Usage tips
Video ports	The number of video ports that are being used in any active conferences. The second number is the maximum number of video ports on this TelePresence Server.	
Audio ports	The number of audio-only ports that are being used in any active conferences. The second number is the maximum number of audio-only ports on this TelePresence Server.	
Content ports	The number of ports that are being used for the content channel in any active conferences. The second number is the maximum number of content ports on this TelePresence Server.	For more information about the content channel, see Content channel video support.

Understanding the Conference controller

It is possible to set up multiple TelePresence Servers to be controlled by a single TelePresence Server, which is then the *Conference controller*. This feature allows you to share a single set of endpoint, conference and room configurations across multiple TelePresence Servers and monitor them from a single TelePresence Server.

Note: The Conference controlling arrangement is not the same as the clustering arrangement of multiple TelePresence Servers. For more information, see Comparing clustering with Conference controlling.

A conference controller controls the calls and conferences on one or more TelePresence Servers. A TelePresence Server that is not a Conference controller will not control calls or conferences on any TelePresence Servers including itself: it has relinquished control to another TelePresence Server.

Using the Conference controller approach has the following consequences:

- All calls must be made to the address of the TelePresence Server that is the Conference controller. This TelePresence Server then decides which TelePresence Server in its system will host each conference.
- Calls to a TelePresence Server that is not a Conference controller are not accepted.
- You must log in to the Conference controller to see status and statistics information for the whole system under its control.
- If the Conference controller fails, conferences running on one of the controlled TelePresence Servers will continue **until** you configure a new Conference controller, which resets all conferences in the system.
- You should regularly back up the configuration of the Conference controller. Then, if it fails, you can restore the configuration to another TelePresence Server to act as Conference controller without having to reconfigure the endpoints, conferences and rooms for the new system. See Backing up and restoring the configuration
- Each TelePresence Server has a certain number of screen licenses, and each screen license effectively activates one video port. The Conference controller can use all the screen licenses for the controlled TelePresence Servers. See Understanding screen licenses .
- If you are using the enhanced font on the Conference controller, you should also upload it to all controlled TelePresence Servers to ensure consistent experience across all hosted conferences.

Configuring a single TelePresence Server system

If you are running a single TelePresence Server system, the TelePresence Server must be configured as a Conference controller:

1. Go to **Configuration > System settings**.
2. For **Conference control**, select *Conference controller - this system will manage all conferences*.
3. Click **Apply changes**.
   This TelePresence Server will now control all calls and conferences.

Configuring a multiple TelePresence Server system

To create a multiple TelePresence Server system, create a Conference controller and then add the controlled TelePresence Servers via its web interface:

1. Log in to the TelePresence Server that will be the Conference controller and go to **Configuration > System settings**.

2. For **Conference control**, select *Conference controller - this system will manage all conferences*.
3. Click **Apply changes**.
4. On each of the TelePresence Servers that will be controlled, set **Conference control** to *Conferences will be managed by an external controller*.
5. Go to **TelePresence Servers > Add new TelePresence Server**.
6. Enter the name, address and port numbers of a controlled TelePresence Server. See Adding and configuring TelePresence Servers for more details.
7. Click **Add new TelePresence Server**.
8. Add any other controlled TelePresence Servers in the same way.

To check communication between the Conference controller and the controlled TelePresence Servers, go to **TelePresence Servers** on the Conference controller and check that the **Status** of each controlled system is *OK*.

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. For more information about screen licenses, see Understanding screen licenses.

Note: The Conference controlling arrangement is not the same as the clustering arrangement of multiple TelePresence Servers. For more information, see Comparing clustering with Conference controlling.

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 16 screen licenses, the cluster has 64 video ports. The master can allocate them as necessary, for example, all in one large conference, or distributed across several smaller conferences.

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.
- No guest logins / users are allowed on slave blades; they only have admin logins.
- You cannot upload / delete the enhanced font file on a slave blade; it is only required by the master.

Comparing clustering with Conference controlling

There are two overlapping concepts for arranging multiple TelePresence Servers. One way is to create a cluster of TelePresence Servers, in which one is master and up to three are slaves; the other option is to nominate one or more additional TelePresence Serverto be under the control of a TelePresence Server called the Conference controller.

These two concepts are not mutually exclusive, and you can mix them when you arrange multiple TelePresence Servers. The following rules apply:

- There is only ever one Conference controller in a system of controlled TelePresence Servers.
- If there is only one TelePresence Server in a system, then that one must be the Conference controller.
- One or more clusters may be controlled by another TelePresence Server; the cluster does not need to be the controller.
- If a cluster is to be the Conference controller, then the master blade must be the Conference controller; a slave blade can never be a Conference controller.

For more on clusters, see Understanding clustering . For more on Conference controllers, Understanding the Conference controller.

This table summarizes the differences between the two arrangements:

Differences between Clustering and Conference control

Comparison value	Clustering notes	Conference controller notes
Hardware support	Clustering is only possible on Cisco TelePresence Server MSE 8710 blades. You can not cluster Cisco TelePresence Server 7000 series servers.	Conference controller functionality is in all TelePresence Servers and can be used between Cisco TS MSE 8710 blades and Cisco TS 7000 series servers; a blade can control a server or a server can control a blade.
Licensing	Requires a *Cluster support* feature key, copied to each blade in the cluster.	Does not require a feature key.
Co-location	Clustered blades must reside in the same MSE 8000 chassis.	A Conference controller can control remote TelePresence Servers.
Load balancing allowed	Yes	Yes
Pooled screen licenses	Yes	Yes
Resource allocation	The master may allocate resources from one clustered TelePresence Server to a conference hosted on another. This means that the maximum conference size is limited either by the pooled number of licenses, or by the available capacity of the whole cluster - whichever is consumed first by the conference.	The Conference controller may only allocate resources to a conference on a server-local basis; that is, the maximum conference size is limited to the number of participants supported by the TelePresence Server that the Conference controller allocates to the conference.

Comparison value	Clustering notes	Conference controller notes
Conference control	Master controls conferences and decides how to allocate resources within the cluster.	Conference controller controls all conferences, and decides which TelePresence Server, or cluster, hosts each.
Calls in	Calls must come into the master blade, unless it is not the Conference controller; slave blades cannot respond.	Calls must always come in to the Conference controller.

Understanding screen licenses

Each TelePresence Server has a certain number of screen licenses, and each screen license effectively activates one video port. If you have fewer screen licenses than the number of video ports provided, then not all of those video ports will be available for use by calls between the TelePresence Server and video conferencing endpoints. When all screen licenses are in use, the TelePresence Server will use audio-only ports for additional calls, and so those new calls will not be able to contribute or see video.

With multiple TelePresence Server devices working together, activated screen licenses on the Conference controller and its controlled TelePresence Servers are effectively pooled so that the number of available screen licenses is the sum of the available screen licenses of all the TelePresence Servers. For maximum flexibility, the Conference controller TelePresence Server can reallocate screen licenses between TelePresence Servers, provided that the allocated screen licenses do not exceed the combined total.

With multiple TelePresence Server devices clustered together, activated screen licenses are effectively pooled and allocated to the master blade in the cluster so that the number of available screen licenses is the sum of available screen licenses in the cluster.

You must have a screen license key, provided by your supplier, to activate screen licenses.

- For TelePresence Server 8710 blades housed in a Cisco TelePresence MSE 8000 chassis, you configure the screen license key on the Supervisor blade and then allocate licenses to the individual TelePresence Server 8710 blades.
- For TelePresence Servers that operate as standalone units, enter the screen license keys on **Configuration > Upgrade** in the same way as you add feature keys.

Rooms

Displaying the rooms list

Note: The **Rooms >** pages are only available if your TelePresence Server has the *Third party interop* feature key installed. You can see which keys are installed on **Configuration > Upgrade**.

You can configure rooms on the TelePresence Server so that users can create ad hoc conferences from the endpoints associated with the corresponding physical rooms.

The **Rooms** page displays all the rooms are configured on the TelePresence Server. The list is sorted alphabetically by name by default; click any column heading to sort by that column.

From the Rooms list you can:

- Click on a room name to see its status.
- Add a new room.
- Select and delete one or more rooms.

The following details are displayed for each room.

Room list details

Field	Field description
Name	The name of the room.
User ID	The username of the room's account.
Endpoint	The endpoint or endpoint group that is associated with the room. You can also click an endpoint or endpoint group name to see its status page.

Displaying room status

A room's **Status** page provides details of the conference activity for that room. To access a room's status page, go to **Rooms** then click the room's name.

This page tells you if the room's conference:

- is active and how many endpoints are in the conference
- is registered to a gatekeeper or registrar
- is locked
- has port limits, and what they are
- includes a content channel
- had previous participants and who they were

From this page you can also:

- Call one or more endpoints: To do this, select the endpoints from the list and click **Call endpoint**. Alternatively, click **Call endpoint** and enter the IP address, URI, or E.164 number. Note that you cannot call an endpoint group in this way and the gatekeeper will only be used if **Use gatekeeper** has been enabled on the **Configuration > System settings** page.
- End an active conference: To do this, click **Disconnect all**
- Disconnect one or more endpoints: To do this, select the endpoints and click **Disconnect selected**
- Send a message to all participants: Click **Send message**, type in the message and click **Send message**. This message appears overlaid on each participant's view.

  Note: Depending on the viewing screen, very long messages might not display properly. Therefore, consider limiting messages to a few hundred characters. The message is displayed in the middle of the screen for approximately 30 seconds.

The following information is displayed for each conference:

Status

Field	Field description	Usage tips
Status	The activity status of the conference.	Conferences can be: ■ *Active (<X> endpoints)* while there are active participants . ■ *Inactive*: there is currently no conference started by this room.

Field	Field description	Usage tips
H.323 gatekeeper status	The status of a conference with respect to its H.323 gatekeeper.	One of: ■ *Numeric ID registered* ■ *Numeric ID failed to register* ■ *Not registered:* conference is not configured to register with the gatekeeper ■ *Registering*: conference is in the process of registering If the TelePresence Server can connect to an H.323 gatekeeper, the name and numeric ID of a conference can be registered with that gatekeeper as a different directory number. This allows H.323 users to dial directly into a particular conference. To configure a H.323 gatekeeper, go to **Configuration > System settings**.
SIP registrar status	The status of a conference with respect to its SIP registrar.	One of: ■ *Numeric ID registered* ■ *Numeric ID failed to register* ■ *Numeric ID unable to register (registration settings not configured)* conference is configured to try and register but it cannot because the system's SIP call configuration is set to *Use trunk* or *Call direct* instead of *Use registrar* ■ *Not registered:* conference is not configured to register with the registrar ■ *Registering*: conference is in the process of registering If the TelePresence Server can connect to a SIP registrar, the name and numeric ID of a conference can be registered with that gatekeeper as a different directory number. This allows users to dial directly into a particular conference. To configure a SIP registrar , go to **Configuration > System settings**.
Content	Whether the content channel is currently in use.	One of: ■ *Disabled*: content sharing is disabled for this room. To enable content for this room, go to **Rooms > *Room name* > Configuration** ■ *No current presentation:* content sharing is enabled for the room but there is no active contributor ■ *Presentation from <endpoint display name>*: there is an active contributor of content For more information, see Content channel video 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: ■ *In conference* ■ *Joining conference* ■ *No endpoints*: there is no conference running from this room

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 endpoint may have disconnected for one of the following reasons: ■ *unspecified error*: the endpoint has disconnected, but the TelePresence Server does not know the reason ■ *no answer*: the endpoint has failed to connect because it did not answer ■ *call rejected*: the endpoint has failed to connect because it rejected the call ■ *busy*: the endpoint has failed to connect because it was busy ■ *gatekeeper error*: the endpoint has failed to connect because of a gatekeeper error ■ *left conference*: the endpoint has left the conference ■ *destination unreachable*: the endpoint has failed to connect because it was unreachable The TelePresence Server may have disconnected the endpoint for one of the following reasons: ■ *requested by administrator*: the endpoint has been disconnected by an administrator ■ *requested via API*: the endpoint has been disconnected via the API ■ *end of conference*: the endpoint has been disconnected at the end of a conference ■ *requested via web interface*: the endpoint has been disconnected via the web interface ■ *encryption unsupported*: the endpoint has been disconnected because it does not support encryption ■ *deleted*: the endpoint has been disconnected because the endpoint was deleted ■ *conference deleted*: the endpoint has been disconnected because the conference was deleted ■ *group disconnect*: the endpoint has been disconnected because a group member disconnected ■ *TIP failed*: the endpoint has been disconnected because TIP negotiation failed ■ *no free resources*: the endpoint has been disconnected because there are no free resources ■ *configuration change*: the endpoint has been disconnected because of a configuration change ■ *disconnect timeout*: the endpoint has been

Field	Field description	Usage tips
		disconnected (timeout) ■ *TS deleted*: the endpoint has been disconnected because the hosting TelePresence Server has been deleted ■ *moved conference*: the TelePresence Server has disconnected the endpoint to move it to another conference

Adding and configuring rooms

Note: The **Rooms >** pages are only available if your TelePresence Server has the *Third party interop* feature key installed. You can see which keys are installed on **Configuration > Upgrade**.

Each room has an endpoint and a user account associated with it. A users who log into the TelePresence Server with this account can create a conference that includes the room's endpoint. The user can invite other endpoints or endpoint groups that you have selected for use with this room.

Adding a new room

1. Go to **Rooms > Add new room**.
2. Supply the room details, referring to the following table if necessary.
3. Click **Add new room**.
   The room exists now but you stay on the configuration page so you can add pre-configured endpoints.
4. Click **Add pre-configured participants**.
5. Select endpoints that this room will be able to invite into ad hoc conferences.
6. Click **Update conference**.
   The list of **Pre-configured participants** now shows all the endpoints that users from this room can call into ad hoc conferences.

Updating a room

1. Go to **Rooms**.
2. Click the name of the room you want to update.
3. Modify the details as required, referring to the following table if necessary.
4. Click **Modify room**.

Room configuration reference

Room general settings

Field	Field description	Usage tips
Name	The name of the room.	Enter a name. This will show in the room list.
User ID	The **User ID** that will be used to log in to the TelePresence Server room.	The user will log in to the TelePresence Server web interface using this User ID and the password (described below).
Password	The **Password** that will be used to log in to the TelePresence Server room.	The user will log in to the TelePresence Server web interface using this password. **Note**: When updating a room's configuration, the **Password** field is not editable. To change the password, click **Change password**.
Endpoint	The endpoint or endpoint group to be associated with this room.	All configured endpoints and endpoint groups with valid call-out parameters are listed.
Allow call-out to user-supplied address	Allow the room's user to invite endpoints or endpoint groups that are not pre-configured to join the ad hoc conference.	When enabled, this feature allows the user to enter an H.323 ID or IP address to call a participant who was not previously selected to join conferences started from this room.
Add all endpoints to conference	Make all the endpoints known to the TelePresence Server available to the room.	When the user is creating a conference from the room, the user can select from the TelePresence Server's whole list of pre-configured endpoints. If disabled (default), the room can only invite from the list of **Pre-configured participants** on its own **Configuration** page.

Room conference settings

Field	Field description	Usage tips
Numeric ID	The numeric identifier for conferences created from this room.	See **Register numeric ID with H.323 gatekeeper** and **Register numeric ID with SIP registrar**.
Register numeric ID with H.323 gatekeeper	Allows a conference created from this room to register its Numeric ID with the TelePresence Server's H.323 gatekeeper.	The H.323 gatekeeper is configured on the **Configuration > System settings** page. The room's associated endpoint must be in the conference before other endpoints or endpoint groups can join.
Register numeric ID with SIP registrar	Allows a conference created from this room to register its Numeric ID with the TelePresence Server's SIP registrar.	The SIP registrar is configured on the **Configuration > System settings** page. The room's associated endpoint must be in the conference before other endpoints or endpoint groups can join.

Field	Field description	Usage tips
Conference locked	Locks any conferences started from this room.	Check the box to lock all conferences started from this room. A locked conference prevents participants that have not been invited from joining the conference. A locked room can call out to invite participants in.
Encryption	Whether encryption is *Optional* or *Required* for conferences started from this room.	If encryption is *Required*, only endpoints and endpoint groups that support encryption can join this conference. Encryption requires a feature key. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server.
Use OneTable mode when appropriate	Whether to use OneTable mode. Choose from: ■ *Disabled* ■ *4 person mode* ■ *2 person mode* OneTable mode requires three or more participants which support the OneTable feature.	OneTable mode provides a layout that allows conferences held between locations to be represented as though the participants in each location were seated along one side of the same table. In OneTable mode, each of the three screens of a three-screen endpoint is used to represent one side of the table. For more information, see Understanding how participants display in layout views.
Content channel	Allows conferences created from this room to support an additional video stream for showing content.	Content is typically high resolution, low frame rate video such as a deck of slides. Content can originate from: ■ an endpoint contributing a separate video stream. ■ the TelePresence Server being configured to use an endpoint's main video stream as the conference's content channel. For more information, see Content channel support.
Pre-configured participants	Click **Add pre-configured participants**. This will list all endpoints configured on this TelePresence Server. Select the endpoints or endpoint groups to be available to users of this room. When creating a conference, users will only be able to call endpoints or endpoint groups configured for that room.	The list only shows for existing rooms. If you enable **Add all endpoints to conference**, then all the endpoints that are currently configured on the TelePresence Server are automatically included in this list. You can not edit the list while that option is enabled. If **Add all endpoints to conference**is disabled (default), then you can: ■ select individual endpoints to be visible to the room's user. ■ select/deselect all endpoints by using the check box in the heading row.

Starting a conference from a room

A user can start an ad hoc conference by logging in to the TelePresence Server using a room account. Conferences started this way appear in the format **`conference name (room name)`** on the **Conferences** page.

The room account is associated with a particular endpoint - probably in the corresponding physical room - and may usually invite other endpoints to join a conference.

You must provide the user with the following:

- The IP address of the TelePresence Server.

  Note: Only the Conference controller can connect conferences through a room. If your TelePresence Servers are clustered, then this is the master blade. For more information about the Conference controller, see Understanding the Conference controller. For more information about clustering, Understanding clustering .

- The username and password of the room account.
- The following instructions - also available in the online help after the user logs in.

Log into the room

1. Open a web browser.
2. Enter the IP address of the TelePresence Server.
3. Enter your room's **Username** and **Password**.
4. Click **Log in**.

Start a conference

When you log into the TelePresence Server, you'll see a list of endpoints or endpoint groups that you may invite to join your conference:

1. Select the endpoints or endpoint groups that you want to participate in the conference.
   You may also be able to call an endpoint that is not on the list; if so, you'll see an item labeled with *Enter an address* rather than with a name or address. Check the box and enter the address of the endpoint you want to invite.
2. Click **Call**.
   The conference is now active. You can participate using the endpoint associated with your room. You can also control the endpoints from the web interface (see below).
3. To end this conference, click **End**.

Endpoint controls

While the conference is active, you can use the web interface to control the endpoints that are participating:

Endpoint controls in a room's web interface

Button	Function
	Invite the endpoint.
	Disconnect the endpoint.
	Mute or unmute the participant's video stream.
	Mute or unmute the participant's audio stream.
	Click the endpoint picture to make that participant important; the TelePresence Server will display this participant as prominently as possible.

Room user instructions

Log into the room

1. Open a web browser.
2. Enter the IP address of the TelePresence Server.
3. Enter your room's **Username** and **Password**.
4. Click **Log in**.

Start a conference

When you log into the TelePresence Server, you'll see a list of endpoints or endpoint groups that you may invite to join your conference:

1. Select the endpoints or endpoint groups that you want to participate in the conference.
   You may also be able to call an endpoint that is not on the list; if so, you'll see an item labeled with *Enter an address* rather than with a name or address. Check the box and enter the address of the endpoint you want to invite.
2. Click **Call**.
   The conference is now active. You can participate using the endpoint associated with your room. You can also control the endpoints from the web interface (see below).
3. To end this conference, click **End**.

Endpoint controls

While the conference is active, you can use the web interface to control the endpoints that are participating:

Endpoint controls in a room's web interface

Button	Function
	Invite the endpoint.
	Disconnect the endpoint.
	Mute or unmute the participant's video stream.
	Mute or unmute the participant's audio stream.
	Click the endpoint picture to make that participant important; the TelePresence Server will display this participant as prominently as possible.

Note: The conference cannot continue if you leave the conference. However, the conference continues while you are connected even if other endpoints leave.

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 that the user needs to access the web interface of 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, so may not be present).
Privilege	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 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: You should not modify the event capture filter unless 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**.

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: You should not modify this filter unless you are doing so with advice from a support representative.

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** dropdown.
   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 the support team 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're 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 we 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, simply 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're 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** if you wish to process the log in your text editor, or archive it for future reference. This button *downloads all the records* currently stored on the box; 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** if you want 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 pertaining to a particular conference display this identifier, which can make auditing conference events much simpler. Click the GUID to see only those records that pertain 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.

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, if necessary, 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.
Source identifier	A string that the source will provide to the receiver when it is queried or when it publishes feedback events.	The string is optional and defaults to the MAC address of Ethernet port A on the TelePresence Server.

Reference

Content channel support

Most telepresence endpoints support the use of a second video channel known as the content channel. This is typically 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.

Although the content channel is enabled system-wide by default, the TelePresence Server must cater for endpoints that do not support the second video channel. Go to **Configuration > System settings** and **Allow content in main video**.

With this feature selected, 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 largest pane and other participants' video streams are centered continuous presence panes across the bottom of the display).

Content sharing is enabled by default. To edit this setting for a conference, go to **Conferences > *conference name* > Configuration** and find the **Content channel** setting.

In each conference, only one participant can send a content channel video stream at a time. To enable another participant to become the presenter, either the active presenter must stop sending content or the TelePresence Server must allow participants to take over the content channel.

Content channel configuration settings

When you add a new conference or configure an existing conference, you can choose whether the content channel is allowed in that conference with the **Content channel** setting.

The **Content channel** is *Enabled* for conferences by default, which means that participants are able to contribute content channel video for the other conference participants to see.

If the conference's **Content channel** is *Disabled*, content sharing is not allowed and no participants can contribute content.

For a participant to contribute a content channel requires the following:

- That participant's endpoint must be configured to allow content channel video contribution:
  1. Go to **Endpoints** and then click the participant's endpoint.
  2. Click **[Configuration]**
  3. Check the box labeled **Content video contribution**.
- Either the participant must be the only active presenter or the TelePresence Server must allow automatic content handover:
  1. Go to **Configuration > System settings**.
  2. Check the box labeled **Automatic content handover**.

For a participant to see the shared content on a single-screen endpoint, the endpoint must support content sharing, or have **Allow content in main video** enabled.

The TelePresence Server sends the content channel to one endpoint in an endpoint group; that endpoint must support the content channel:

To choose which endpoint in the group receives the content channel video:

1. Go to **Endpoints** and click the endpoint group name.
2. Click **[Advanced settings]**.
3. Select the endpoint number from the dropdown labeled **Screen to receive content / audio**.
4. Click **Update endpoint**.

Understanding how participants display in layout views

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. 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

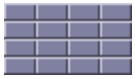
A single-screen TelePresence endpoint always receives the panel switched view when possible, but a participant can change the layout using Far End Camera Control.

In panel switched view, 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 panel switched view 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 System T3 for example).

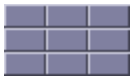
If the panel switched view is not possible, the TelePresence Server composes the layout for single-screen endpoints according to the following rules:

Layouts sent to single screen endpoints if panel switched view is not possible



If there are any four-screen TelePresence systems in a conference, the TelePresence Server sends this layout to single-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 remote systems with fewer screens.

	If there are no four-screen TelePresence systems in the conference but there are three-screen systems, the TelePresence Server sends this layout to single screen systems in that conference Each row of three panes can either show the three screens of a remote three-screen system or a combination of remote systems with fewer screens.
	If there are only single-screen or dual-screen systems in the conference, the TelePresence Server sends this layout to the single-screen systems. Each of the two rows of two panes can either show a remote two-screen system or two single-screen systems.
	If the single-screen participants in a conference are receiving content in the main video channel, the TelePresence Server composes the content and continuous presence panes like this. The content is displayed in the large area at the top and the other participants' video streams are overlaid and centered across the bottom of the screen.

Layouts sent to two-screen systems

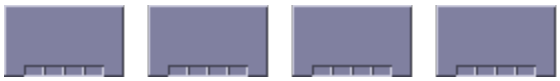
Layouts sent to two-screen systems	
 	If there are any three- or four-screen TelePresence systems in a conference, the TelePresence Server sends this layout to two-screen systems in that conference. Each row of four panes can either show the four screens of a remote four-screen system or a combination 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 are automatically centered if possible.
 	The TelePresence Serveruses this layout if there are only one- or two- screen systems in the conference but it needs more small panes to show the participants.

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 people 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 *2 person mode* or *4 person mode*.

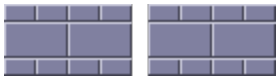
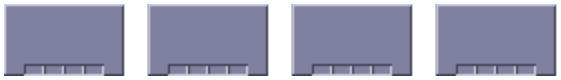
2 person mode: The TelePresence Server composes the participant video streams as if there were two people sitting next to each other on one side of a table, irrespective of their physical location.

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).

When deciding dynamically between different layouts based on the number of small panes available and the number of streams to show, the TelePresence Server does not consider any video streams being received from the viewing system. As an example, the TelePresence Server will not dynamically switch from this layout:

to this layout:

if the only benefit of the additional small panes would be that it was then possible for the participant to see himself/herself.

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:

whereas the following layout is used if all participants are connected via one and two screen systems.

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, with 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.

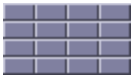
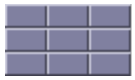
Equally, if you select a setting of *3 screens wide* and a four-screen endpoint joins the conference, the view will change to the one above.

Show continuous presence panes setting

Most multi-screen conference layouts, for example:

consist of a set of full screen panes plus a number of overlaid smaller panes. These overlaid smaller panes are known as continuous presence panes because they allow the TelePresence Server to continuously show all participants that are present. You can choose whether or not to display the continuous presence panes by selecting **Show continuous presence panes**.

For single-screen systems, the following three conference layouts sent by the TelePresence Server do not include any continuous presence panes; all panes are of equal size in these layouts.


The **Show continuous presence panes** setting does still have an effect for single screen systems, however, because the layout used when in OneTable mode uses overlaid continuous presence panes and the presence of the 3 small overlaid panes at the base of the screen is controlled by this option. The overlaid panes are automatically centered if possible.

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 don't support the extra channel.

Endpoints that would otherwise be unable to see the content channel can see it if you enable this feature.

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 overlaid panes; it does not draw borders around participants being shown in large 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.

Ports allocation

Each TelePresence Server unit has a limited number of video ports, audio-only ports and content ports. The following table details how these ports are allocated for the different definition modes supported by the software.

Port allocations by hardware type

Hardware arrangement	Audio-only ports	Content ports	Video ports (HD mode)	Video ports (Full HD mode)
7010	10	10	16	12
8710	10	10	16	12
Cluster of 2 8710s	20	20	32	24
Cluster of 3 8710s	30	30	48	36
Cluster of 4 8710s	40	40	64	48

Endpoint types

Note: Cisco CTS software version 1.7.4 is being developed and tested concurrently with version 2.2 of the Cisco TelePresence Server software. TelePresence Server 2.2 software refers to the current (1.7.3) and earlier versions of the CTS software as 'legacy Cisco CTS' to distinguish them from the imminent version, 1.7.4 (and later versions), which, together with TelePresence Server 2.2, fixes a number of historical interoperability issues.

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)
Telepresence	A single screen telepresence endpoint
TANDBERG T1 or TANDBERG single screen TelePresence	Cisco TelePresence System T1 (formerly TANDBERG Telepresence T1)
TANDBERG Experia	The TANDBERG Experia
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
Cisco telepresence	An unknown type of Cisco CTS system, running legacy software (CTS 1.6 / 1.7 up to 1.7.3)
Cisco single screen telepresence	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
Cisco three screen telepresence	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 system running CTS 1.7.4 or later
SIP single screen TelePresence	A Cisco CTS single screen system running CTS 1.7.4 or later, for example: ■ CTS 500 ■ CTS 1000 ■ CTS 1100

Endpoint type (shown in UI)	Hardware names / model numbers
SIP three screen TelePresence	A Cisco CTS 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)
-	The endpoint type is not recognized by the TelePresence Server

Endpoint interoperability

Endpoint feature support

Feature	Endpoints that support this	Notes
Reveal loudest participant for panel switched layout	T3, CTS 3200, CTS 3000	CTS 1300 and endpoint groups do not reveal the loudest participant.
Add legacy Cisco CTS 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 Cisco CTS 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 more recent versions of the CTS software (1.7.4).
Conference ending notification	■ CTS 500 ■ CTS 1000 ■ CTS 1100 ■ CTS 1300 ■ CTS 3000 ■ CTS 3010 ■ CTS 3200 ■ CTS 3210	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.

Checking for updates and getting help

We recommend registering your product at http://www.tandberg.com/services/video-conferencing-product-registration.jsp in order to receive notifications about the latest software and security updates. New feature and maintenance releases are published regularly, and we recommend that your software is always kept up to date.

If you experience any problems when configuring or using the product, consult the documentation at http://www.tandberg.com/support/video-conferencing-documentation.jsp for an explanation of how its individual features and settings work. You can also check the support site at http://www.tandberg.com/support/ to make sure you are running the latest software version.

You or your reseller can also get help from our support team by raising a case at http://www.tandberg.com/support/. Make sure you have the following information ready:

- The software build number which can be found in the product user interface (if applicable).
- Your contact email address or telephone number.
- The serial number of the hardware unit (if applicable).

Contact details and license information

Please refer to the following sections for details of where to get further help and for additional software license information:

TANDBERG

TANDBERG is now part of Cisco.

For further assistance and updates visit the TANDBERG web site: www.tandberg.com

Software licenses

This product can use HMAC-SHA1 to authenticate packets and AES to encrypt them.

The following copyright notices are reproduced here in order to comply with the terms of the respective licenses.

NetBSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: *This product includes software developed by the NetBSD Foundation, Inc. and its contributors.*
4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- The University of California, Berkeley and its contributors.
- The University of California, Lawrence Berkeley Laboratory and its contributors.
- The NetBSD Foundation, Inc. and its contributors.
- Jonathan R. Stone, Manuel Bouyer, Charles M. Hannum, Christopher G. Demetriou, TooLs GmbH, Terrence R. Lambert, Theo de Raadt, Christos Zoulas, Paul Kranenburg, Adam Glass, Winning Strategies, Inc, Frank van der Linden, Jason R. Thorpe, Chris Provenzano.

Info-ZIP

Copyright © 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Independent JPEG Group's JPEG software

TANDBERG Codian software is based in part on the work of the Independent JPEG Group

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright © 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

1. If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.
2. If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".
3. Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

The OpenSSL Project

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

AES License

Copyright (c) 2001, Dr Brian Gladman, Worcester, UK.

All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and fitness for purpose.

Issue Date: 29/07/2002

HMAC License

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 26/08/2003

SHA1 License

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 01/08/2005

Lua

Lua 5.0 license

Copyright © 2003-2004 Tecgraf, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

1. The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DHCP

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of ISC, ISC DHCP, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTERNET SYSTEMS CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ISC OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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.