Cisco TelePresence Server on Multiparty Media 820

Printable Online Help

First Published: August 2016

Software version:4.4

Contents

Introduction

This document contains the text of the online help for the Cisco TelePresence Server version 4.4 web user interface. It is provided so that the help text can be viewed or printed as a single document.

This document accompanies version 4.4 of the TelePresence Server software as installed and used on the Cisco TelePresence Server on Multiparty Media 820.

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

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

Further Information

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

Logging into the Web Interface

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

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

There are three privilege levels for user accounts:

- *Administrator*: users with this privilege level may access all functionality
- *API access*: users with this privilege level can only access the API, not the web interface
- *None*: users with this privilege level may not access the TelePresence Server. This level is used to disable accounts.

Tasks

Logging in to the web interface:

1. Enter the host name or IP address of the TelePresence Server into the address bar of a web browser.

   The log in page displays.
2. Enter your assigned **Username** and **Password**.
3. Click **OK**.

Failing to Log into the Web Interface

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

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

- **Invalid username/password**: you have typed the incorrect username and/or password.
- **No free sessions**: the maximum number of sessions allowed simultaneously on the TelePresence Server has been reached.
- **Your IP address does not match that of the browser cookie you supplied**: try deleting your cookies and log in again
- **You do not have access rights to view this page**: you do not have the access rights necessary to view the page that you attempted to see

- **Page expired**: the **Change password** page can expire if the TelePresence Server detects that the user who requested to change password, may not actually be the user submitting the change password request. (This may happen if you use a new browser tab to submit the request.)

System Status

Displaying System Status

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

Note: Your TelePresence Server must be controlled by an external application. The external application, for example Cisco TelePresence Conductor, uses the TelePresence Server's API to create and manage conferences and participants. Refer to the Cisco TelePresence Server API documentation for more information.

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

Table 1 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.	
License mode	Indicates whether the TelePresence Server is operating in Screen Licensed mode (default) or Multiparty Licensed mode.	To enter Multiparty Licensed mode the TelePresence Server must be in remotely managed mode, have no active calls and be connected to a TelePresence Conductor with Multiparty Licensed mode activated.

Table 2 Feature keys

Field	Field description	Usage tips
Media 820 activation	Whether or not the unit is enabled.	The TelePresence Server will not operate without activation. This feature key is installed before shipping.
Media encryption	Whether or not media encryption is enabled.	The *Media encryption* feature key allows encrypted conferences on this TelePresence Server. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server. **Note**: If you are using a TelePresence Conductor older than XC4.0 and do not have the Media encryption key installed, TelePresence Conductor will display a warning that the encryption key is required. This warning is erroneous.
Cluster support	This feature allows Media 820 blades configured on the same Cisco TelePresence MSE 8000 chassis to be linked together to behave as a single unit.	Up to two blades can form a cluster. See Understanding clustering. If you want to cluster blades, each blade must have the *Cluster support* feature key installed. Feature keys are installed on the **Configuration > Upgrade** page. See Upgrading and backing up the TelePresence Server
Screen licenses	The number of screen licenses allocated to the TelePresence Server. In the case of a cluster, this is the number of screen licenses allocated to the whole cluster. The number of allocated screen licenses can be lower than the maximum that the system can support.	You need to install a screen license key to enable screen licenses. For more information about licenses, see Understanding your TelePresence Server's Conferencing Capacity, page 67.

Table 3 Conference status

Field	Field description	Usage tips
Active conferences	The number of active conferences on this TelePresence Server.	A conference is active if it has participants.
Active participants	The number of participants (of all types) that are currently in conferences on this TelePresence Server.	
Previous participants	The number of participants who were previously participating in a conference (since the last time the TelePresence Server restarted).	

Table 4 System log

Field	Field description	Usage tips
	The system log displays the most recent shutdown and upgrade events, with the most recent shown first.	

Table 5 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 your TelePresence Server, provide this file to the Cisco Technical Assistance Center (TAC) who may wish to perform further diagnostic tests.
Network capture file	To download a network capture, click **Download file**.	There is also a link to **Delete network capture** which you should only click when your TelePresence Server is operating normally again.
System logs	To download the logs, click **Download file**.	An archive containing several useful log files.

Displaying Hardware Health Status

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

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

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

Table 6 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.

Table 6 Device health details (continued)

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

Displaying Cluster Status on a Master TelePresence Server

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

The table below describes the **Status > Cluster** page that displays for the master TelePresence Server in a cluster. For details about slave blades, see Displaying Cluster Status on a Slave TelePresence Server, page 11.

Table 7 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 slave, or *Master blade* in the case of the master.	You can click the IP address to go to the slave's cluster page.

Table 7 Cluster status (continued)

Field	Field description	Usage tips
Status	The status of the master can only be *OK* which means that the master is operating correctly in the cluster. The following options are possible for slave status: ▪ *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 rejoin the cluster. Wait a few minutes and then refresh the **Status > Cluster** page. ▪ *Still starting up*: The slave 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 rejoin the cluster. Wait a few minutes and then refresh the **Status > Cluster** page. ▪ *Failed, version mismatch*: All TelePresence Servers in the cluster must be running the same version of software. This status message indicates that this slave is running different software to the master, and hence the TelePresence Server is not part of the cluster. Update all units in the cluster to the same version of the software.	If the status of the slave is OK, it is currently functioning in the cluster. For any of the other statuses, the slave is not currently functioning as part of the cluster. If a slave has a problem that causes it to no longer be part of the cluster, the cluster can continue to operate without the slave. If a slave fails, participants in conferences will not be disconnected: if there are sufficient resources in the cluster, they will continue to receive audio and video. In the worst case, participants may lose video. The audio will continue because all audio is processed by the master. If the master loses contact with a slave, the slave will automatically restart itself. In this way, it can rejoin the cluster.
Software version	The software version on each TelePresence Server in the cluster.	
Media processing load	An overview of the current media loading of each TelePresence Server in the cluster. The load may increase during periods of peak conference use.	Conferences are distributed between the TelePresence Servers in the cluster. The load on each depends on the number and size of the conferences running on them.
Screen licenses	The number of screen licenses on each TelePresence Server in this cluster.	All screen licenses on slaves are controlled by the master. It does not matter to the cluster how you allocate the screen licenses–the master controls all screen licenses and even if a slave fails, the master will continue to have access to any screen licenses allocated to the failed slave.

Displaying Cluster Status on a Slave TelePresence Server

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

The table below describes the **Status > Cluster** page that displays for slave TelePresence Servers in a cluster. For information about the master TelePresence Server, see Displaying Cluster Status on a Master TelePresence Server , page 10.

Slave units have restricted user interfaces; not all settings are available.

Table 8 Cluster status

Field	Field description	Usage tips
Status	Possible statuses for the master unit are: ■ *Still starting up*: the master 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 has lost contact with the master. This status will only be momentarily visible because the slave will quickly restart itself in this case.	If a slave TelePresence Server loses contact with the master, it will restart itself. This is the only way that a slave can correctly rejoin the cluster. A common reason for a slave to lose contact with the master is because the master has restarted.
Last seen	This field is only visible if the master has not been seen for up to 11 seconds. The slave will automatically restart itself shortly after it loses contact with the master.	
IP address	The IP address of the master TelePresence Server.	

Network Settings

Configuring Network Settings

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

On this page:

- IP Configuration Settings, page 13
- IP status, page 14
- Ethernet configuration, page 15
- Ethernet status, page 15

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**.

Table 9 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.	You can disable IPv4 on the TelePresence Server port but only if logged in using IPv6.
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify this option if you have chosen *Manual* IP configuration, as described above. For Port A, if the IP configuration setting is set to *Automatic by DHCP* this setting will be ignored.

Table 9 IPv4 configuration (continued)

Field	Field description	Usage tips
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	

Table 10 IPv6 configuration

Field	Field description	Usage tips
IP configuration	Select *Disabled*, *Automatic via SLAAC/DHCPv6* or *Manual*. If you select *Manual*, you must also supply the IPv6 address, prefix length and default gateway. If you select *Automatic via SLAAC/DHCPv6*, the TelePresence Server automatically gets an IPv6 address. It uses SLAAC, Stateful DHCPv6 or Stateless DHCPv6 as indicated by the ICMPv6 Router Advertisement (RA) messages (see Automatic IPv6 address preferences below).	Disable IPv6 on the port if the network does not support IPv6. You can disable IPv6 on the TelePresence Server port but only if logged in using IPv4.
IPv6 address	If you chose *Manual* configuration, supply the IPv6 address in CIDR format, for example `fe80::202:b3ff:fe1e:8329`.	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**.

Table 11 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. Select *Automatic* negotiation if you require a connection speed of *1000 Mbit/s*.
Speed	(For *Manual* configuration only) Set the connection's speed to *100 Mbit/s*.	The connection speed setting must be the same for the ports at both ends of this connection.
Duplex	(For *Manual* configuration only) Set the connection's duplex mode to *Full 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.

Ethernet status

Table 12 Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether or not this Ethernet link is connected.	
Speed	The speed 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 of the network connection to this port.	This value is Full Duplex, either negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value can not be changed, it is for information only.
Packets sent	The total number of packets sent from this port (all TCP and UDP traffic).	This information can help you confirm that the TelePresence Server is transmitting packets into the network.
Packets received	The total number of packets received by this port (all TCP and UDP traffic).	This information can help you confirm that the TelePresence Server is receiving packets from the network.

Table 12 Ethernet status (continued)

Field	Field description	Usage tips
Statistics:	More statistics for this port. ■ Multicast packets sent ■ Multicast packets received ■ Total bytes sent ■ Total bytes received ■ Receive queue drops ■ Collisions ■ Transmit errors ■ Receive errors	This information can assist you with diagnosing network issues, such as link speed and duplex negotiation issues.

Configuring DNS Settings

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

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

Table 13 DNS settings

Field	Field description	Usage tips
DNS configuration	Select how you want the TelePresence Server to get its name server address. For example, if you select *Via Port A DHCPv6*, the device will automatically get a name server address using DHCP over the IPv6 network connected to Ethernet port A. If you select *Manual*, you must provide a name server address. You may also want to provide a secondary name server or domain name (DNS suffix).	The TelePresence Server does not allow you to automatically configure the name server address if you have set a static IP address on the selected interface. For example, if you select *Via Port A DHCPv4* here but have also selected *Manual* in the IPv4 configuration section of the **Port A settings** page, the TelePresence Server will warn you that no DNS servers will be configured.
Host name	Specifies a name for the TelePresence Server.	The host name can be up to a maximum of 63 characters. 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 when **DNS configuration** is *Manual*.
Secondary name server	Identifies an optional second name server.	If an optional second name server is configured, the TelePresence Server may send DNS queries to either name server.

Table 13 DNS settings (continued)

Field	Field description	Usage tips
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 to create these routes correctly as failure to do so may result in you being unable to make calls or access the web.

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

On this page:

- IP routes configuration
- Current routes tables

IP Routes Configuration

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

Add a New IP Route

To add a new route:

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

Use the following table for reference:

Table 14 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).	IPv4 example: To route all IPv4 addresses in the range 192.168.4.128 to 192.168.4.255, specify the IP address as 192.168.4.128 and the mask length as 25. The first 25 bits are fixed, which means that the last seven bits determine the range of addresses. IPv6 example: To route all IPv6 addresses in the range 2001:db8::0000 to 2001:db8::ffff, enter the IP address 2001:db8:: and the mask length as 112. The first 112 bits are fixed, which means that the last 16 bits determine the range of addresses.
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	You may select *Port A*, or *Gateway*. If you select *Gateway*, enter the IP address of the gateway to which you want packets to be directed. If you select *Port A*, matching packets will be routed to Port A's default gateway (see Configuring network settings).

To View or Delete an Existing IP Route

The page displays the following details for each route:

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

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

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

Current Routes Tables

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

Configuring IP Services

Go to **Network > Services** to control access to the web services on the TelePresence Server.

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

Enabling TCP/UDP Services

There are options to control IPv4 and/or IPv6 services, depending on which IP versions are enabled on the **Network > Network settings** page.

1. Check the boxes next to the service names you want to enable, or clear the boxes to disable services.
2. Edit the port numbers for the services if necessary.

   (Commonly used port values are entered by default).
3. Click **Apply changes**.

Defining the Ephemeral Port Range

Note: The lowest ephemeral port must be greater than the highest configured TCP or UDP service port. For example, if HTTPS was set to port 20000 then the lowest ephemeral port allowable is 20001.

1. Enter the Minimum port number in your preferred ephemeral port range.

   The default is 49152. The minimum port cannot be set to be below 10000.
2. Enter the Maximum port number in your preferred ephemeral port range.

   The default is 65535 which is the maximum possible setting, giving a default range of about 15000 ports. The TelePresence Server will not allow you to reduce the range below 5000 ports because this would potentially hamper conferencing functionality.
3. Click **Apply changes**.
4. If you want to reset the values to their default settings, click **Reset to default** and then click **Apply changes**.

Resetting to the Default Configuration

1. Click **Reset to default**.

   The TelePresence Server replaces any changed settings with the page defaults. These do not take effect immediately.
2. Click **Apply changes**.

   The default settings take effect.

Table 15 Network > Services field descriptions

Field	Field description	Usage tips
HTTP	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.
HTTPS	Enable/disable secure (HTTPS) web access on the specified interface or change the port that is used for this service.	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.
SIP (TCP)	Allow/reject incoming calls to the TelePresence Server using SIP over TCP or change the port that is used for this service.	

Table 15 Network > Services field descriptions (continued)

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.	
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.
Minimum	The lower limit of the ephemeral port range.	Defaults to 49152, though you can set it as low as 10000 or as high as 60535.
Maximum	The upper limit of the ephemeral port range.	Defaults to 65535, though you can set it as low as 15000. The minimum range is limited to 5000 ports.

Configuring QoS Settings

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

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

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

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

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

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

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

On this page:

About QoS Configuration Settings

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

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

Table 16 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.

Table 17 IPv6 configuration

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

ToS Configuration

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

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

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

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

DiffServ Configuration

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

Default Settings

The default settings for QoS are:

- **Audio** *101110*:
  - For ToS, this means IP precedence is set to 5 giving relatively high priority. Delay is set to low, throughput is set to high, and reliability is set to normal.
  - For Diff Serv, this means expedited forwarding.

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

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

Configuring SSL Certificates

If you enable HTTPS on the **Network > Services** page (enabled by default), you will be able to access the web interface of the TelePresence Server using HTTPS.

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

The Cisco TelePresence Server has a local certificate and private key pre-installed that it uses 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. We recommend a key length of between 2048 bits and 8192 bits.

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

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

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

To upload your own certificate and key, go to **Network > SSL certificates**.

Note: DTLS is only negotiated if your TelePresence Server has the *Media encryption* feature key.

Complete the fields using the table below for help and click **Upload certificate and key**. Note that you must upload a certificate and key simultaneously. You must restart the Cisco TelePresence Server after uploading a new certificate and key.

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

The store may contain multiple certificates. This can be achieved by uploading a single trust store file containing multiple PEM encoded certification authority certificates one after another within the normal BEGIN and END certificate tags.

You can remove your own certificate and key, if necessary, by clicking **Delete custom certificate and key**. You must restart the TelePresence Server after deleting a certificate.

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

Table 18 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.	
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.

Table 19 Local certificate configuration

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

Table 20 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.	

Table 21 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 `flex.participant.requestDiagnostics`)	Browse to and select the trust store certificate file, then click **Upload trust store**. The store may contain multiple certificates. When verification is required (see following setting) the certificate of the remote party is verified against the trust store: the remote certificate must either be in the trust store or in the trust chain of one of its certificates. Click **Delete trust store** if you need to remove it or replace it with an updated file.
Certificate verification settings	Determines the circumstances in which the remote certificate must be verified with the trust store.	Select one of the drop-down options below and click **Apply changes**. ■ *No verification*: The remote certificate is never verified against the trust store (remote end always trusted). ■ *Outgoing connections only*: The TelePresence Server attempts to verify the remote certificate for all outgoing SIP TLS and HTTPS connections. ■ *Outgoing connections and incoming calls*: The TelePresence Server attempts to verify the remote certificate for all incoming and outgoing SIP TLS connections, and for outgoing HTTPS connections. **Note**: A maximum of 12 subjectAltNames are supported if certificate verification is enabled.

Testing Network Connectivity

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

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

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

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

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

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

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

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

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

Viewing Network Statistics (netstat)

Go to **Network > Netstat** to view the current status of all TCP and UDP connections to the TelePresence Server.

The netstat data refreshes each time you load or refresh the UI page, or when you click **Refresh**, or when you check or clear the **Resolve names** checkbox.

Table 22 Netstat field descriptions

Field	Description
Resolve names	Check the box to perform a DNS lookup on the addresses and show hostnames if possible, or clear the box to show the IP addresses instead. The data refreshes when you toggle the checkbox.
Protocol	*tcp4*, *tcp6*, *udp4*, or *udp6*, indicating which internet protocol and addressing scheme the connection is using.
Recv-Q	Count of bytes queued on this connection because they have not yet been processed by the TelePresence Server.
Send-Q	Count of bytes queued on this connection because they have not yet been acknowledged by the remote party.
Local Address	The address of the TelePresence Server on this connection. If **Resolve names** is not checked this field shows the local socket as `address:port`. If **Resolve names** is checked it shows the socket as `hostname:servicename` if possible. Eg. `ts.example.com:http` or `127.0.0.1:80`

Table 22 Netstat field descriptions (continued)

Field	Description
Foreign Address	The address of the remote party on this connection. If **Resolve names** is not checked this field shows the foreign socket as `address:port`. If **Resolve names** is checked it shows the socket as `hostname:servicename` if possible. Eg. `browser.example.com:http` or `192.168.3.1:80`
State	The state of the connection. For more information, see http://tools.ietf.org/html/rfc793#section-3.2
Service	The name of the service that the TelePresence Server provides on this connection. The service name is hyperlinked to the **Network > Services** page so you can change the service configuration if necessary.

Configuration

Configuring System Settings

To modify the system settings, go to **Configuration > System settings**, edit the fields (see table for details), and then click **Apply changes**.

Most conference configuration defaults are made using the management system, for example TelePresence Conductor.

Table 23 Settings for all configured conferences

Field	Field description	Usage tips
Display video preview images	When checked, thumbnail preview images of conference participants' video streams are shown on the TelePresence Server user interface.	The default is enabled (checked).
Show event log messages on console	Check the box to enable event log output to the serial console, or clear the box to disable event log output to the serial console. Your selection persists if the TelePresence Server restarts. When the checkbox is cleared, the TelePresence Server will still output event log messages to the serial console from the time it powers up until the media resources are available. After this time, the TelePresence Server stops sending event log messages to the console.	The checkbox is cleared by default which means that serial output of the event log is disabled. This default helps to improve the TelePresence Server's performance, so there may be a performance impact If you enable this setting. We recommend that you use a syslog server to capture event log messages. See Logging Using Syslog, page 51.
Disable serial console input during startup	Check the box to prevent the TelePresence Server from interpreting anything from the console while it is starting up.	We recommend that you check this box to prevent console users from interrupting the normal boot sequence .

Table 23 Settings for all configured conferences (continued)

Field	Field description	Usage tips
Require administrator login for serial console commands	Check the box to prevent the TelePresence Server from interpreting console commands unless the user has been identified.	We recommend that you check this box to secure the serial console against unauthorised users who have gained physical access. **Note:** The TelePresence Server's console cannot accept all Unicode characters. Accounts used for console access are limited to ASCII characters for username and password.
Idle serial console session timeout	Number of minutes that the TelePresence Server will maintain an open console session after the last input.	We recommend that you use a short value to avoid leaving unattended console sessions open to unauthorised users.

Configuring SIP Settings

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

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

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

Table 24 SIP

Field	Field description	Usage tips
Outbound call configuration		*Use trunk*: ■ Directs outbound SIP calls via the trunk to the SIP server address you provide. ■ The SIP server, for example Cisco Video Communication Server (VCS) or Cisco Unified Call Manager (CUCM), is responsible for the onward routing of outbound SIP calls from the TelePresence Server. *Call direct*: ■ The TelePresence Server will connect SIP calls directly if possible. It does not use the **Outbound address** or **Outbound domain** parameters. ■ The TelePresence Server does not attempt to use the trunk.
Outbound address	The hostname or IP address of the SIP registrar or trunk destination.	The TelePresence Server ignores this field if **Outbound call configuration** is set to *Call direct*.

Table 24 SIP (continued)

Field	Field description	Usage tips
Outbound domain	The domain of the trunk destination.	The TelePresence Server ignores this field if **Outbound call configuration** is set to *Call direct*. The TelePresence Server uses this value for any outbound SIP calls where the supplied address does not contain an @ symbol. If you do not specify an outbound domain, the TelePresence Server uses the outbound address instead.
Username	The TelePresence Server uses this name to authenticate with the SIP device (trunk destination or endpoint) if that device requires authentication.	
Password	The TelePresence Server uses this password to authenticate with the SIP device (trunk destination or endpoint) if that device requires authentication.	The SIP destination may not require authentication; if it does, you need to configure it to accept a log in from this username and password combination.
Outbound transport	Select the protocol that the TelePresence Server will use for outbound calls. One of *TCP*, *UDP*, or *TLS*.	The TelePresence Server uses this protocol for communicating with the trunk destination. If you have the encryption feature key installed and want to encrypt signaling, select *TLS*. The TelePresence Server accepts incoming connections on whichever protocol the connection uses (TCP, UDP or TLS), and will respond using the same protocol, irrespective of this **Outbound transport** setting. Make sure that you enable those services on the **Network > Services** page.
Advertise Dual IPv4/IPv6	Select *Use ANAT* if you want the TelePresence Server to support SIP calls in a mixed IPv4 and IPv6 network.	Default is *Disabled*. When configured to use ANAT (Alternative Network Address Types), the device supports ANAT syntax in the session description. See http://tools.ietf.org/html/rfc4091 for more information.

Table 24 SIP (continued)

Field	Field description	Usage tips
Negotiate SRTP using SDES	Select whether the TelePresence Server will negotiate SRTP using SDES for either of the following options: ▪ *For secure transports (TLS) only* ▪ *For all transports*. (Note: this parameter only displays with the *Media encryption* feature key.)	The TelePresence Server supports the use of encryption with SIP. When encryption is in use with SIP, the audio and video media are encrypted using Secure Real-time Transport Protocol (SRTP). When using SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDES). SDES exchanges keys in clear text, so it is a good idea to use SRTP in conjunction with a secure transport for call control messages. You can configure the TelePresence Server to also use Transport Layer Security (TLS) which is a secure transport mechanism that can be used for SIP call control messages. The default setting is *For secure transports (TLS) only*.

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

System Time

Current time displays the time according to the TelePresence Server.

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.

Table 25 Device time settings

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

Using NTP over NAT (Network Address Translation)

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

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

Backing Up and Upgrading the TelePresence Server

On this page:

Upgrading the Main TelePresence Server Software Image

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

To upgrade the main TelePresence Server software image:

1. Go to **Configuration > Upgrade**.
2. Check the **Current version** of the main software image to verify the currently installed version.
3. Log onto the support pages to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the TelePresence Server web browser interface.
7. Go to **Configuration > Upgrade**.
8. Locate the unzipped file on your hard drive.

   The button may be **Browse...** or **Choose File** or similar, depending on your browser.
9. Click **Upload software image**. The browser begins uploading the file to the TelePresence Server, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
10. The upgrade status displays in the **TelePresence Server software upgrade status** field.
11. Shut down and restart the TelePresence Server.

Backing Up and Restoring the Configuration

The Back up and restore section of the **Configuration > Upgrade** page allows you to back up and restore the configuration of the TelePresence Server using the web interface. This enables you to either revert to a previous configuration 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. Go to **Configuration > Upgrade**.
2. Locate and select a previously-saved configuration.xml file.

   The button may be **Browse...** or **Choose File** or similar, depending on your browser.

3. 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.
4. Click **Restore backup file**.

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

- If you check **Network settings**, the network configuration will be overwritten with the network settings in the supplied file.

  Typically, you would only select this check box if you are restoring from a file backed up from the same TelePresence Server or if you are intending to replace an out of service TelePresence Server.

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

Enabling TelePresence Server Features

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

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

Each key is unique to a particular TelePresence Server. Ensure that you know the device's serial number when you request the key, so that the supplier can give you a valid key.

Applying the key is the same process whether you are activating the TelePresence Server or enabling an advanced feature.

To apply a key to the TelePresence Server:

1. Read the **Feature management** list to check whether the feature is already active.

   The product activation key is also in this list.
2. Enter the key given to you by your supplier into the **Add key** field *exactly as you received it*, including any dashes.
3. Click **Add key**.

   The browser window refreshes to list the newly added feature and the key you entered.

   If the key is not valid, you are prompted to re-enter it.

   Keys 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 keys remain in the list even though the corresponding features disabled.
4. Record the key 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 key, to remove a feature.

Applying Screen Licenses

To license a TelePresence Server, you must log in to the Supervisor and allocate screen licenses to the blade slot. The screen licenses are linked to the chassis serial number. See the Supervisor documentation for details.

Shutting Down and Restarting the TelePresence Server

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

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

To shut down the TelePresence Server:

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

   The button changes to **Confirm TelePresence Server shutdown**.
3. Click the button again to confirm.

   The TelePresence Server will begin to shut down. The banner at the top of the page will change to indicate this.

   When the shutdown is complete, the button changes to **Restart TelePresence Server**.
4. Click this button a final time to restart the TelePresence Server.

Changing the Administrator Password

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

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

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

Conferences

Displaying the Conference List

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

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

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

On this page you can:

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

The list contains the following information for each conference:

Table 26 Conference list details

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

Table 26 Conference list details (continued)

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

Displaying Conference Status

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

From this page you can tell whether the conference:

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

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

- Select and then **Disconnect selected** participants
- **Disconnect all** participants, effectively ending the conference
-
- 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

Table 27 Status

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

Table 28 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.	
Authority	Either *Chair* or *Guest*, to indicate the participant's role (and associated authority) in the conference.	This defaults to *Chair* for all participants unless the managing system has explicitly applied chair/guest control levels to this conference.
Status	The status of the endpoint.	One of: ▪ *Joining conference*: the endpoint is joining this conference ▪ *In conference*: the endpoint is currently participating in this conference. ▪ *Attempting to re-establish call*: the endpoint is busy and a retry is occurring. Additional status information may be displayed, for example, *xx failed to join* (grouped endpoints), *packet loss detected*, *video to muted*, *video from muted*, *video muted* (and the equivalent for audio), *important*, and *audio-only*. If a pre-configured endpoint is busy when the conference starts, the TelePresence Server will retry the endpoint up to five times throughout the conference and connect if and when it becomes free. The retry intervals are 5, 15, 30, 60 and 120 seconds.
More...	Click **More...** to see previews of the transmit and receive streams. You can also control the endpoint's contribution to the conference. Click **[Expand / Collapse All]** to show more status information for all endpoints in the list.	You can: mute  and unmute  audio mute  and unmute  video make a participant important (transmit stream only)  or unimportant 

Table 29 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.	

Table 29 Previous participants (continued)

Field	Field description	Usage tips
Reason for disconnection	Why the endpoint is no longer part of the conference.	The TelePresence Server may have disconnected the endpoint for one of the following example reasons: ■ *requested by administrator*: the endpoint has been disconnected by an administrator. ■ *call rejected*: the far end rejected the call. ■ *left conference*: the endpoint has been disconnected at the end of a conference. ■ *requested via API*: the endpoint has been disconnected via the API. ■ *no answer*: the endpoint did not answer the call. ■ *busy*: the endpoint has failed to connect because it was busy (for SIP calls this could also mean that the endpoint rejected the call). ■ *destination unreachable* The endpoint was unreachable. ■ *Encryption not supported by far end*: encryption required for the call but the far end does not support it or encryption forbidden for this call but far end requires encryption. ■ *timeout*: Connection timed out. ■ *insufficient free ports*: the endpoint has been disconnected because there are insufficient free ports. ■ *conference port limit reached*: the endpoint has been disconnected because the conference port limit has been reached. ■ *Conference locked*: the call could not connect to the conference as it is locked. ■ *Product not activated*: the call could not be made/accepted as there is no activation key installed on the TelePresence Server. ■ *Protocol error*: the endpoint has been disconnected due to a protocol error. ■ *Network error*: the endpoint has been disconnected due to a network error. ■ *Unavailable*: the endpoint is unavailable.

Table 29 Previous participants (continued)

Field	Field description	Usage tips
		■ *Capability negotiation error*: the endpoint and the TelePresence Server are unable to negotiate a mutually compatible call set up. ■ *Insufficient token allocation*: the token specification/allocation was not sufficient for TIP/MUX call. ■ *TIP/MUX negotiation failure*: the endpoint has been disconnected because TIP/MUX negotiation failed to complete successfully. ■ *No media received*: The TelePresence Server disconnected this endpoint because at least 30 seconds have passed since it unexpectedly stopped sending media. ■ *unspecified error*: the endpoint has disconnected, but the TelePresence Server does not know the reason.

Displaying Endpoint and Group Status

The endpoint status is only available when the endpoint is part of an active conference in Remotely Managed mode. You can control the endpoint to some extent from here.

1. Go to **Conference** and select the **Status** page
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.

Table 30 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 is currently connected or not).
Manufacturer code		
Product		
Version		

Table 31 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.

Table 31 Status (continued)

Field	Field description	Usage tips
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. SIP.	
Endpoint advertised capabilities	The capabilities that the endpoint advertised when negotiating the call.	For example: Audio, Video, Video content, Encrypted traffic, Unencrypted traffic.
Audio channels	Whether receive and transmit audio channels are open between the Cisco TelePresence Server and the far end.	
Video channels	Whether receive and transmit video channels are open between the Cisco TelePresence Server and the far end.	
Extended video channels	Whether receive and transmit extended video channels are open between the Cisco TelePresence Server and the far end.	
Received audio gain mode	The audio gain mode that is configured, on the endpoint, for audio received from the TelePresence Server. One of *<use default>*, *Automatic*, *Fixed*, or *Disabled*.	*<use default>*: This endpoint has inherited the Automatic Gain Control setting of the conference. *Automatic*: The TelePresence Server dynamically adjusts the gain of the audio received by this endpoint to approximate the levels received by the other participants. *Disabled*: Gain control is disabled for the audio received by this endpoint. *Fixed*: The TelePresence Server adjusts the endpoint's received audio by a fixed ratio. This is configured in the **Received audio gain** field on the endpoint's settings page.
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.
Preview	Sample stills of the video stream (s).	The preview shows a still from each screen for both the receive stream and the transmit stream aligned under the appropriate direction and bandwidth used figure. You can click to refresh the preview.
Endpoint *X*	(Endpoint groups only) The connection status of each endpoint in an endpoint group.	
Duration	The time that the endpoint/endpoint group has been in this conference.	

Table 31 Status (continued)

Field	Field description	Usage tips
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. This button is disabled for multistream endpoints.	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.
Send message	Click to send a message to the endpoint.The **Send message** page displays: 1. Enter your message and a duration (in seconds) for the message to display. 2. Click **Send message**.	This button is only enabled for multistream endpoints under the following circumstances: - The endpoint must be ActiveControl capable. - The endpoint must subscribe to messages. - The conference must have messaging enabled.

Viewing Endpoint or Endpoint Group Statistics

1. Go to **Conference** and select the **Status** page.
2. Click on the endpoint or group name. The endpoint's **Status** page displays.

3. Click **Statistics** to view the **Endpoint Statistics** page.

   The information is displayed in up to four sections: **Audio**, **Auxiliary audio**, **Video**, and **Content channel**.

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

4. The data automatically updates every 3 seconds. However, you can also manually update the data by refreshing the page in your browser, or click **Refresh**, to get the latest statistics.

For multiscreen endpoints you are directed to the **Multiscreen Stream Selection** page. Select the desired stream to go to the **Endpoint Statistics** page where you will see data for all the streams associated with that channel.

Multistream endpoints have up to four receive and 16 transmit video streams.The individual video, audio, and content streams for a multistream endpoint are displayed as follows: **Rx Audio**, **Tx Audio**, **Rx Video**, **Tx Video**, and **Content**. Select a stream on the **Multistream Stream Selection** page to view the **Endpoint Statistics** page for the selected stream only.

Note: Selecting a multiscreen channel displays data for all the streams associated with that channel, whereas for multistream endpoints—because the streams are independent of one another and there are more of them—you must select an individual stream and the **Endpoint Statistics** page displays data for that stream only.

Note: Statistics for multistream calls can take a few seconds to load.

Table 32 Receive stream statistics

Field	Field description
Receive stream	The codec used in the received stream. For video and content channels, this also shows the dimensions of the video stream.
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/video/content packets that have been received by the Cisco TelePresence Server. The second number indicates 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 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.

Table 32 Receive stream statistics (continued)

Field	Field description
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.
ClearPath FEC	Statistics on the Forward Error Correction (FEC) used in this stream. The value is *Not supported* if the endpoint cannot apply FEC to the stream, or cannot negotiate ActiveControl with the TelePresence Server. Otherwise, there are two statistics: the percentage overhead and the number of packets recovered. The percentage overhead measures how many FEC packets are inserted compared to the original stream. If the endpoint inserts a copy of every packet in the stream, the overhead is 100%. If the endpoint inserts a copy of every second packet, the overhead is 50%, and for every fourth packet, 25%. The real statistics will not always perfectly match these levels, owing to the counting interval and timing of RTCP reports. The number of packets recovered is a simple count of packets recovered by the TelePresence Server from the endpoint's FEC packets because the originals were lost.
ClearPath LTRF	Reports *N repair frames received* if LTRF (Long Term Reference Frames) is enabled. This indicates the number of times LTRF has been used in the stream.

Table 33 Transmit stream statistics

Field	Field description
Transmit stream	The codec used in the transmitted stream. For video and content channels, this also shows the dimensions of the video stream.
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 / reported lost	The number of audio/video/content packets destined for the endpoint. The second number is the number of those packets that the endpoint did not receive, as reported by 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.

Table 33 Transmit stream statistics (continued)

Field	Field description
ClearPath FEC	Statistics on the Forward Error Correction used in this stream. There are two statistics: the percentage overhead and the number of packets reported recovered. The percentage overhead measures how many FEC packets are inserted compared to the original stream. If the TelePresence Server inserts a copy of every packet in the stream, the overhead is 100%. If the TelePresence Server inserts a copy of every second packet, the overhead is 50%, and for every fourth packet, 25%. If the TelePresence Server is not currently applying FEC to this stream, then the overhead is 0%. The figure is the number of packets reported recovered by the endpoint from the TelePresence Server's FEC packets because the originals were lost.
ClearPath LTRF	Whether Long Term Reference Frames are used in this stream. The value is *Not supported* if the endpoint cannot negotiate ActiveControl with the TelePresence Server. Otherwise, the value is *Enabled*, which means that LTRFs are sent to the endpoint and can be used if necessary.

Users

Displaying the User List

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

Table 34 User list details

Field	Field description
User ID	The user name needed to access the web interface of the TelePresence Server. You can enter text in whichever character set you require, however, note that some clients do not support Unicode characters.
Name	The name of the user (optional, so may not be present).
Access rights	The role and associated permissions granted to this user. There are three levels: *Administrator*, *API access*, and *None*. *None*: this user is locked out of the TelePresence Server. *API access*: this user may run API commands at this TelePresence Server's XML-RPC interface. *Administrator*: has API access and administrative access to the web interface.

Deleting Users

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

Adding and Updating Users

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

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

Adding a User

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

Updating a User

1. Go to **Users**.
2. Click a User ID.

3. Modify the user account details, referring to the following table if necessary.
4. Click **Modify user**.
5. If you need to change the password, click **Change password**.

User Details Reference

Table 35 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 clients do not support Unicode characters. **Note:** The TelePresence Server's console cannot accept all Unicode characters. Accounts used for console access are limited to ASCII characters for username and password.
Name	The name of the user.	Optional.
Password	Type a password for this user.	Although you can enter text in whichever character set you require, note that some clients do not support Unicode characters.
Re-enter password	Retype the password.	The password entry fields are only active by default when you add a new user. If you are updating an existing user, click **Change password** to enable editing in these fields.
Access rights	Choose a role for the user from the dropdown. The roles grant permissions as follows: *None*: this user is locked out of the TelePresence Server. *API access*: this user may run API commands at this TelePresence Server's XML-RPC interface. *Administrator*: has API access and administrative access to the web interface.	

Logs

Working with 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 all the system logs in a single zip file: click **Download system logs**.
- Download the event log as text: go to **Logs > Event log** and click **Download event log**.
- 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 **Logs > Event capture filter** page.

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

- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Logs > Syslog** page.
- Empty the log by clicking **Clear event 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: Only modify this filter if doing so with advice from Customer Support.

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

1. Go to **Logs > Event capture filter**.
2. Select *Detailed trace* from the **VIDEO** drop-down list.

   The TelePresence Server warns you that performance may be affected.
3. Click **OK** (this is a temporary elevation in detail that you can reverse after your issue is resolved).
4. Click **Update settings**.

   The TelePresence Server will capture detailed trace information from the video sub-system, as well as the default information for all other sub-systems.

Event Display Filter

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

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

Message 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.

Current 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 Protocols Messages

The **Protocols log** page records the messages received by or transmitted from the TelePresence Server for a variety of protocols.

Protocols logging is disabled by default because the volume of messages affects performance, but Customer Support may ask you to enable it to assist in troubleshooting.

If you wish to start logging protocols messages:

1. Select which protocols you wish to log.
2. Click **Enable protocols logging** to start recording these protocol messages.
3. Perform the tests required to reproduce the issue you are trying to resolve.
4. Click **Download as XML** to get the log as an XML file to send to support.

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

Field	Description
Current status	*Enabled* or *Disabled*. *Disabled* by default.
Messages logged	Count of messages logged.
Protocol filters	▪ *BFCP* ▪ *SIP* ▪ *XCCP* Check the boxes for the protocol messages you want to capture. These are capture filters, not display filters; when you uncheck a protocol and then enable protocols logging, the TelePresence Server does not capture any messages for the unchecked protocols. You cannot change which protocols are logged while logging is enabled. If you want to change the capture filters, disable logging, change the checkboxes, then enable logging again.

Remote Logging of Protocols Messages

The protocols log is available over HTTP or HTTPS, thus allowing the log to be recorded to a remote device. The setting to enable or disable protocols logging does not disable sending the log to a remote device. A maximum of two simultaneous log streams are available at any time.

If you wish to start logging protocols messages to a remote device:

1. Send an HTTP POST request from the remote device to `http[s]://<ip address>/protocols_log_stream`. This POST request must include the following valid user and password parameters:
   `authenticationUser=username&authenticationPassword=password`.

   The following is an example using wget (for a Linux system):
   `wget https://<IP address>/protocols_log_stream --post-data=authenticationUser=username&authenticationPassword=password`

   (Users with API-only permissions are considered valid.)

2. The entire contents of the protocols log is then streamed back to the remote device using this TCP connection. The log stream continues until the remote device breaks the TCP connection.

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:

Table 36 Syslog settings

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

Using Syslog

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

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

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

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

Working with Call Detail Records

The TelePresence Server web interface can display up to 1000 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.

Note: The TelePresence Server can store up to 2000 Call Detail Records and these can be viewed by downloading the XML. See below.

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, page 53
- Call Detail Record Log, page 54

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:

Table 37 Status and display

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

Call Detail Record Log

The Call Detail Record log displays as a long table on a single page and includes up to 1000 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).

Click **Download as XML** to process the log in your text editor, archive it for future reference, or view up to 2000 Call Detail Records. This button *downloads all the records* currently stored; it ignores any display filters you have set on the web page.

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

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

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

CDR Log Reference

The following table describes the fields in the CDR log:

Table 38 CDR log details

Field	Field description	Usage tips
# (record number)	The unique index number for this Call Detail Record.	
Time	The time at which the Call Detail Record was created.	Records are created as different conference events occur. The time the record was created is the time that the event occurred. Incoming CDR log events are stored with the local time stamp (not UTC). Changing the time (either by changing the system time or via an NTP update) causes new events in the CDR log to show the new time. No change will be made to the timestamp of existing records.
Conference	The GUID of the conference to which this record applies.	Each new conference is created with a globally unique identifier (GUID). All records relating to a particular conference display this identifier, which can make auditing conference events much simpler. Click the GUID to see only those records that relate to this conference.
Participant	The GUID of the participant to which this record applies.	Each participant is represented by a globally unique identifier (GUID), which can simplify your record management. Click the GUID to see only those records that pertain to this participant.

Table 38 CDR log details (continued)

Field	Field description	Usage tips
Message	The type of the Call Detail Record, and brief details, if available.	Click **>>** to expand the details of all messages of this type. You can do this for all messages by selecting *All* and clicking **Update display**, which can be useful in combination with the **Filter string** to find records where the message contains a particular word.

API Clients

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

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

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

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

Table 39 API client details

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

Feedback Receivers

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

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

Each receiver in the list has the following details:

Table 40 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.

Using Call Home

Note: The TelePresence Server currently only supports anonymous reporting.

The TelePresence Server can submit reports about its status and any faults that it has experienced to the Cisco Call Home service. The TelePresence Server always uses a secure connection (HTTPS) to transmit reports to Call Home.

When Call Home is disabled (default setting), the device will not send a report of any type until you select a **Call Home mode**. When you have enabled Call Home, you can manually submit a report or configure the feature to work automatically.

Call Home reports are sent to https://tools.cisco.com/its/service/oddce/services/DDCEService. You may need to update your firewall to allow the reports through, by adding the domain `tools.cisco.com` and opening port 443 for outbound TCP traffic.

When you use *Anonymous Call Home*, you will not be able to view anonymously submitted reports; they are only available to Cisco engineers and are only used to diagnose potential issues.

Note: If you have any questions about a Call Home report please contact Cisco TAC.

After choosing the Call Home mode *anonymous*, you can check **Automatic Call Home enabled** if you want the TelePresence Server to automatically submit reports. The device sends any pending reports as soon as you apply this change. After that, it will automatically send diagnostic reports about any unexpected device restarts or media resource restarts without further manual intervention.

If you prefer not to use automatic Call Home, you can click **Call Home now** to manually send reports at any time.

The *Device inventory* report is always available; its presence does not indicate any special condition or fault. If automatic Call Home is enabled, the TelePresence Server always sends these reports on startup.

To configure Call Home:

1. Go to **Logs > Call Home**.
   The **Status** section shows whether this feature is enabled and what reports are currently available.
2. Select the **Call Home mode,** *Anonymous Call Home*.
3. (Optional) Check **Automatic Call Home enabled** if you want the TelePresence Server to submit reports without manual intervention.
4. Click **Apply changes**.
   A dialog displays asking **Are you sure you want to apply configuration changes?**
5. Click **OK** to proceed or **Cancel** to abandon the configuration changes.
   If Automatic Call Home is enabled, the TelePresence Server sends any pending reports now.
6. (Optional) Click **Call Home now** to manually submit the **Current reports**

Table 41 Status fields

Field	Description
Call Home status	Indicates the Call Home status as one of: ■ *Automatic – Anonymous Call Home* – **Call Home mode** is enabled and **Automatic Call Home enabled** is checked. ■ *Enabled – Anonymous Call Home* – **Call Home mode** is enabled and **Automatic Call Home enabled** is unchecked. ■ *Disabled* (default) On start up, if **Call Home mode** is disabled, the TelePresence Server logs this in the event log during start up. The TelePresence Server also logs a message if **Call Home mode** is enabled (*Anonymous Call Home*) but is not configured to automatically submit reports.
Current reports	A list of available reports.
Submission status	Indicates the status of the latest reports submission, including date and time. Status is *Not sent* if no reports have been submitted.
Last submitted report reference	This field only displays if an **Unexpected media resource restart diagnostics** or an **Unexpected device restart diagnostics** report has been sent. This reference number can be provided to Cisco TAC so they can analyze the report.
Call Home now	Manually submits **Current reports**. A confirmation pop-up displays when manually submitting a report or enabling automatic reporting to indicate that data will be transmitted to Cisco. Report submissions are retried 3 times. If a submission fails after the third attempt, a banner displays on the web interface.

Table 42 Configuration fields

Field	Description
Call Home mode	Enables *Anonymous Call Home*. (*Disabled* by default, no reports can be submitted.)
Automatic Call Home enabled	Allows the TelePresence Server to send diagnostic reports when necessary; also allows the TelePresence Server to send inventory reports when it starts up.

Reference

Content Channel Support

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

- SIP systems use a protocol called BFCP for content.
- Cisco CTS systems and other TIP systems use TIP to control content sharing.

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

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. Endpoints can also choose a layout with far-end camera control or DTMF keys 2 and 8 or can be preconfigured to one of the choices below. The TelePresence Server is capable of working with one-, two-, three- and four-screen regular and immersive endpoints, and displaying any combination of those systems participating in a conference to any other type of system in the conference.

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

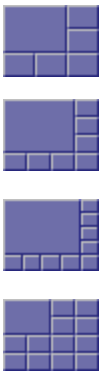
Layouts Sent to Single-Screen Systems

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

In ActivePresence layout, the loudest participant appears full screen with additional participants appearing in up to six equally sized overlaid panes at the bottom of the screen. Any additional participants are indicated by the Participant Overflow Icon.

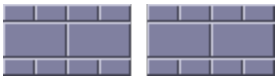
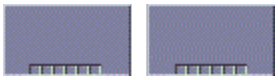
The TelePresence Server composes the layout for single-screen endpoints according to the setting of the **Default layout type for single-screen endpoints**:

Table 43 Layouts sent to single-screen endpoints

	*Single*: Endpoints will be shown in one full screen pane.
	*ActivePresence*: Endpoints will be shown in one full screen pane with additional participants appearing in up to six equally sized overlaid panes at the bottom of the screen. Any additional participants are indicated by the Participant Overflow Icon in the bottom right-hand corner together with the number of unshown participants.
	*Prominent*: Endpoints will be shown in one large pane with additional participants appearing in up to six equally sized panes at the bottom of the screen. Any additional participants are indicated by the Participant Overflow Icon in the bottom right-had corner together with the number of unshown participants.
	*Equal*: Endpoints will be shown in a grid pattern of equally sized panes on the screen, up to 4x4. Each row of panes can either show screens of a remote multi-screen system or a combination of remote systems with fewer screens.
	*OnePlusN layout family*: One larger pane nestled in up to 12 smaller panes. The layout starts as “single” then automatically grows to onePlus5, onePlus7, onePlus9, and onePlus12 based on the number of participants.

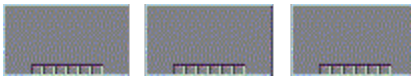
Layouts Sent to Two-Screen Systems

Table 44 Layouts sent to two-screen systems

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

Layouts Sent to Three-Screen Systems

Table 45 Layouts sent to three-screen systems

	Layout without pips is available, i.e. forced to be without pips. DTMF 2 and 8/ FECC can be used to select it.
	When the TelePresence Server is in room-switched display mode, 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.

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 six 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.

Endpoint Configuration Options that Affect View Layouts

Self View Setting

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

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

Show Full-Screen View of Single-Screen Endpoints

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

For single-screen systems, the **Show full screen view of single-screen endpoints** setting determines if/how an endpoint is allowed to be shown in a large full-screen pane. Available settings are *Always*, *Dynamic* and *Disabled*.

- *Always*: Single screen endpoints will always be allowed to occupy a main pane of a multiscreen endpoint.
- *Dynamic*: Single screen endpoints will be visible in the main pane of a multiscreen endpoint if no other multiscreen endpoints are in the conference. If a multiscreen endpoint joins the conference, single screen endpoints will be demoted to the PiP strip.
- *Disabled*: Single screen endpoints will never be shown in the main pane of multiscreen endpoints.

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

Allow Content in Main Video

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

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

Show Borders Around Endpoints Setting

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

The TelePresence Server draws a blue border around the active speaker in the conference, and a grey border in all other cases. 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.

Enhanced Layout Experience

The TelePresence Server supports multistream video. This support is turned off by default.

This means that a multistream-capable endpoint can compose the video streams locally into a conference layout resulting in an enhanced user experience. However, all endpoints continue to be supported with the best experience available to them.

To achieve this, the TelePresence Server advertises the ability to send multiple streams, and allows a multistream-capable endpoint to subscribe to the streams that it requires.

The TelePresence Server can receive up to four main video streams from a multistream-capable endpoint—of the same video source at different resolutions and frame rates, for example, the endpoint could send both 1080p30 and 720p60, or 720p30 and 480p30.

The TelePresence Server can transmit up to eighteen video streams to an endpoint, also at different resolutions and frame rates. A multistream-capable endpoint will then compose the video streams locally into a conference layout.

Some key points to note about this feature:

- Only supported in remotely managed mode on Cisco TelePresence Server on Virtual Machine and Cisco Multiparty Media 310/320.
- The TelePresence Server supports conferences featuring both multistream and single stream endpoints.
- Provides encryption for switched media streams.
- Provides resilience for multistream calls using Forward Error Correction and rate control.
- Multistream is supported via SIP only (not H.323 or TIP).
- It is disabled by default. However, it can be enabled using the API `multistreamMode` parameter.
- The TelePresence Server provides support using an H.264 SVC channel to receive and transmit video streams to and from a multistream-capable endpoint.
- Multistream is not supported over cascade links.
- Multistream is supported for all token levels. However, the main video bit rate must be 500kbps minimum.

Note:

- TIP endpoints are displayed on multistream-capable endpoints by displaying only the active speaker segment.
- All endpoints will be switched to transcoded mode when a grouped endpoint is in a conference.

Endpoint Types

Table 46 Endpoint types

Endpoint type (shown in UI)	Hardware names / model numbers
Standard	Standard video endpoints, for example: ■ EX60 / EX90 ■ Any C-Series codec (C20, C40, C60, C90) ■ Cisco Jabber ■ Microsoft Lync ■ Any other non-TIP 3rd party endpoint Also displays if the endpoint type is unknown to the TelePresence Server
Cascade	A cascade call to another TelePresence Server (Media 310/320, MSE 8710, or Cisco TelePresence Server on Virtual Machine)
Group of N endpoints	A group of endpoints. The list does not contain the individual group members
Legacy TIP endpoint	■ An unknown type of Cisco CTS system, running legacy software (CTS 1.6 / 1.7 up to 1.7.3) ■ 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 ■ A Cisco CTS three screen system, running legacy software (CTS 1.6 / 1.7 up to 1.7.3) for example: – Cisco TelePresence System 3000 series (CTS 30x0) – Cisco TelePresence System 3200 series (CTS 32x0)
SIP telepresence	An unknown type of Cisco CTS or other TIP-capable system running CTS 1.7.4 or later
SIP single screen telepresence	A Cisco CTS or other TIP-capable single screen system running CTS 1.7.4 or later, for example: ■ CTS 500 ■ CTS 1000 ■ CTS 1100
SIP three screen telepresence	A Cisco CTS or other TIP-capable three screen system running CTS 1.7.4 or later, for example: ■ Cisco TelePresence System 3000 series (CTS 30x0) ■ Cisco TelePresence System 3200 series (CTS 32x0) ■ Cisco TelePresence TX9000 ■ Cisco TelePresence TX9200
Multistream	A Cisco supported multistream-capable endpoint.

Endpoint Interoperability

Table 47 Endpoint feature support

Feature	Endpoints that support this	Notes
Reveal loudest participant for panel switched layout	T3, CTS 3200, CTS 3000, TX9000, TX9200	CTS 1300 and endpoint groups do not reveal the loudest participant. **Note**: Some T3 systems cannot provide positional audio, i.e. T3 Custom.
Conference ending notification	▪ CTS 500 ▪ CTS 1000 ▪ CTS 1100 ▪ CTS 1300 ▪ CTS 3000 ▪ CTS 3010 ▪ CTS 3200 ▪ CTS 3210 ▪ TX9000 ▪ TX9200	These endpoints generate their own conference ending warning when they receive notification from the TelePresence Server. They show an icon instead of an overlaid message as seen by other types of endpoints.

Understanding Clustering

A cluster is a group of blades, hosted in 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 license count of both appliances in the cluster. This larger screen count provides you with the flexibility to set up conferences with more participants or several smaller conferences.

Overview of a Cisco TelePresence Server on Media 820 Cluster

Cisco Multiparty Media 820 blades running TelePresence Server software version 4.2 or later support clustering. Currently you can cluster up to two blades, with one blade being the master and the other being the slave.

The master can allocate the cluster's licenses as necessary, for example, all in one large conference, or distributed across several smaller conferences.

See Understanding your TelePresence Server's Conferencing Capacity, page 67 for more information.

Master TelePresence Servers

The screen licenses allocated to each of the TelePresence Servers in a cluster are "inherited" by the master; all the capacity in the cluster is controlled by the master. You must control the cluster's functionality via the master, using either its web interface or its API.

All calls between the cluster and endpoints are made by the master.

Slave TelePresence Servers

Slave TelePresence Servers do not display the full web interface. Some settings pages are available, for example, to configure the network and logging settings, and to upgrade the software.

Similarly, a slave TelePresence Server will not respond to the full complement of API commands. For more information, refer to the relevant API documentation.

Upgrading Clustered TelePresence Servers

When you need to upgrade the TelePresence Server software on all units in a cluster, first upload the new software images to each unit 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:

- The Supervisor must be running a software version **later** than 2.3(1.38) to configure clustering.
- All TelePresence Servers in a cluster must be running identical software builds.
- Each blade in the cluster must have the *Cluster support* feature key.
- You can use any slot in the chassis when clustering the Media 820.
- You cannot cross-cluster between the Media 820 and other types of blade.
- 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 (via Supervisor); 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.

Understanding your TelePresence Server's Conferencing Capacity

This topic includes information for all types of Cisco TelePresence Server. Look for the information that is relevant to your particular model.

License Keys and Screen Licenses

The TelePresence Server's licensing model is based on "screen licenses" , which are purchased and supplied in the form of a license activation key. Screen licenses activate the conferencing capacity for the TelePresence Server. The full capacity of a TelePresence Server is activated by applying the maximum number of licenses, which differs by hardware platform as follows:

Hardware platform	Maximum number of screen licenses
TelePresence Server MSE 8710	12
Cluster of two, three, or four TelePresence Server MSE 8710s	24, 36, or 48 respectively
TelePresence Server 7010	12
TelePresence Server on Media 310	6
Cluster of two TelePresence Servers on Media 310	12
TelePresence Server on Media 320	12
Mixed cluster of TelePresence Servers on Media 310 and Media 320	18
Cluster of two TelePresence Servers on Media 320	24
TelePresence Server on Multiparty Media 820	30
Cluster of two TelePresence Server on Multiparty Media 820	60
TelePresence Server on Virtual Machine (8-core)	4
TelePresence Server on Virtual Machine (8-core, HD)	5
TelePresence Server on Virtual Machine (30 vCPU / High Density VM)	10
TelePresence Server on Media 400v	18
TelePresence Server on Media 410v	32
Cisco Meeting Server 1000	42

When licensing TelePresence Server MSE 8710s or TelePresence Server on Multiparty Media 820, you will apply the license key to the chassis via the Supervisor web interface, and then allocate the screen licenses to the slots that house those blades.

When licensing any of the other platforms, you will apply the license key via the TelePresence Server's own web interface, on the **Configuration > Upgrade** page.

Licensing Clusters

When licensing a cluster of TelePresence Server MSE 8710 blades or TelePresence Server on Multiparty Media 820, we recommend that you allocate licenses to each blade's slot. In practice, the 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 screen licenses allocated to the blades in the cluster.

When licensing a cluster of TelePresence Servers on Media 310/320 platforms, we recommend that you apply a license key to each unit. In practice, the master will control all the licenses even if the slave is down; however, if you want to separate the units in future, or if one fails catastrophically, then you will have independent licensing to cover the units after the cluster is split.

Remotely Managed Mode (all models)

In remotely managed mode, the screen licenses are allocated to calls in a granular way. Each screen license unlocks enough capacity for one full HD call or for a number of lower-resource calls.

Concurrent Call Limits in Remotely Managed Mode

Note: These are the recommended combinations for configuration via TelePresence Conductor. Other combinations are possible but are likely to cost more than expected. For further information see http://docwiki.cisco.com/wiki/Advanced_Resource_Optimization_on_TelePresence_Server.

Table 48 TelePresence Server screen licenses per call for each call type

Call type description			Screen licenses required per call
Main video	Audio	Content	
-	Mono	-	1/52
360p30†	Mono	In main video	⅛
360p30†	Stereo	720p5	¼
480p30	Stereo	In main video	¼
480p30	Stereo	720p5	⅓
720p30	Stereo	720p5	½
720p30	Stereo	720p30	1
1080p30	Stereo	720p15	1
720p60	Stereo	720p15	1
1080p30	Stereo	720p30	1½

Table 48 TelePresence Server screen licenses per call for each call type (continued)

Call type description			Screen licenses required per call
Main video	Audio	Content	
Three-screen 720p30	Multichannel	720p5	1½
Three-screen 720p30	Multichannel	720p30	2
1080p30	Stereo	1080p30	2
Dual-screen 1080p30	Stereo	720p30	2
Three-screen 1080p	Multichannel	720p30	3
Three-screen 1080p	Multichannel	1080p30	4
Four-screen 1080p	Stereo	1080p30	4

† Requires TelePresence Conductor XC2.2 or later.

Table 49 TelePresence Server conferencing capacity on various platforms

Screen licenses required per call		Maximum calls by hardware type (with licenses to provide 100% of capacity)											
	8 Cores VM (8 vCPU)—BE6KMD on M3 servers	8 Cores VM (8 vCPU)—on other servers	Media 310 or MCU 5310	30 vCPU VM ‡	Media 320 or MCU 5320	7010, MSE 8710 or MCU MSE 8510	Media 400v ‡ (30 vCPU) ‡‡	Two appliance cluster	Media 820	Media 410v ‡ (46 vCPU)	CMS 1000 ‡ (70 vCPU)	Four blade cluster with 8710/8510	Media 820 cluster (two blades)
	4 screen licenses	5 screen licenses	6 screen licenses	10 screen licenses	12 screen licenses	12 screen licenses	18 screen licenses	24 screen licenses	30 screen licenses	32 screen licenses	42 screen licenses	48 screen licenses	60 screen licenses
1/52	200*	200*	200*	200*	200*	200*	200*	200*	200*	200*	200*	200*	200*
⅛	33	41	49	81	97	97	145	195	200*	200*	200*	200*	200*
¼	16	20	24	40	48	48	72	97	120	128	168	195	200*
⅓	12	15	18	30	36	36	54	73	90	96	126	146	180
½	8	10	12	20	24	24	36	48	60	64	84	97	120

Table 49 TelePresence Server conferencing capacity on various platforms (continued)

Screen licenses required per call		Maximum calls by hardware type (with licenses to provide 100% of capacity)											
	8 Cores VM (8 vCPU)—BE6KMD on M3 servers	8 Cores VM (8 vCPU)—on other servers	Media 310 or MCU 5310	30 vCPU VM ‡	Media 320 or MCU 5320	7010, MSE 8710 or MCU MSE 8510	Media 400v ‡ (30 vCPU) ‡‡	Two appliance cluster	Media 820	Media 410v ‡ (46 vCPU)	CMS 1000 ‡ (70 vCPU)	Four blade cluster with 8710/8510	Media 820 cluster (two blades)
	4 screen licenses	5 screen licenses	6 screen licenses	10 screen licenses	12 screen licenses	12 screen licenses	18 screen licenses	24 screen licenses	30 screen licenses	32 screen licenses	42 screen licenses	48 screen licenses	60 screen licenses
1	4	5	6	10	12	12	18	24	30	32	42	48	60
1½	2	3	4	6	8	8	12	16	20	21	28	32	40
2	2	2	3	5	6	6	9	12	15	16	21	24	30
3	1	1	2	3	4	4	6	8	10	10	14	16	20
4	1	1	1	2	3	3	4	6	7	8	10	12	15

* 200 is the maximum number of calls on a TelePresence Server. Requires Cisco TelePresence Conductor XC2.3 or later.

‡ To achieve the maximum number of calls, Cisco TelePresence Server on Virtual Machine must be the only VM hosted on the Multiparty Media 400v, 410v, CMS 1000, or 30 vCPU VM. It cannot be co-resident with any other UC application (unlike the 8-core option that runs at 2.4GHz minimum and can be co-resident).

‡‡ Media 400v is configured with 30 vCPUs as per the 30 vCPU VM configuration but it has a higher capacity.

Note: The table above assumes that calls of one type are being used to reach these maximum values. To calculate the total number of licenses required for a variety of concurrent calls, sum the screen licenses required for each concurrent call.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Cisco Legal Information

Cisco Trademark