Cisco TelePresence Server
TS 7010 version 2.1
TS 8710 version 2.1

Online help (printable format)

D14510.02

October 2010

Contents

System status

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

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

Field	Field Description	Usage tips
System status		
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 TANDBERG 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.	
H.323 gatekeeper status	How many Telepresence Servers are registered to an H.323 gatekeeper, and whether the registrations have been made to the primary or an alternate gatekeeper.	This field is only displayed on the Conference controller Telepresence Server and on the master blade in a Telepresence Server cluster.
SIP registrar status	How many Telepresence Servers are registered to a SIP registrar.	This field is only displayed on the Conference controller Telepresence Server and on the master blade in a Telepresence Server cluster.
Conference control	Whether this Telepresence Server is the Conference controller.	Can be: *Conference controller - this system will manage all conferences* *Conferences will be managed by an external controller* For more information, see Understanding the conference controller.
Activated features		
Telepresence Server activation	Whether the blade is enabled as a Telepresence Server or not.	Your blade will not operate without this feature and the key is installed before shipping.

Field	Field Description	Usage tips
Encryption	Whether encryption is enabled on this unit or not.	The encryption feature key allows encrypted conferences and HTTPS web management on this blade. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server.
Third party interop	Whether this unit can be used in Telepresence calls to Telepresence endpoints other than those manufactured by TANDBERG and to grouped endpoints.	This field is only displayed if you have the appropriate key installed. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server.
Licensed ports	The number of licensed video ports in use across all active conferences. The total number of licensed video ports may be less than the total number of video ports supported by the Telepresence Server.	Ports are licensed by installing a screen license function key. For more information about licenses, see Understanding screen licenses. Screen licenses are shared between the Conference controller Telepresence Server and the Telepresence Servers it controls. The value shown here for a Conference controller Telepresence Server is the total number of port licenses for all related Telepresence Servers.
Conference status		
Active Telepresence Servers	If this Telepresence Server is the Conference controller then this field shows the number of Telepresence Servers (including this system) that are being controlled by this Telepresence Server.	A Telepresence Servers can be configured as a Conference controller so that one Telepresence Server can manage conferences across a number of Telepresence Servers. This means you only need to log in and manage one Telepresence Server. The Conference controller shows the number of Telepresence Server systems that it is controlling. A Telepresence Server that is not the Conference controller will show zero here. For more information, see Understanding the Conference controller.
Active conferences	The number of active conferences that this Telepresence Server is controlling.	If this is the Conference controller, then this is the number of active conferences across all managed Telepresence Servers. A Telepresence Server that is not the Conference controller will show zero here. For more information, see Understanding the Conference controller.
Active endpoints	The number of endpoints (of all types) that are in active conferences controlled by this Telepresence Server.	If this is the Conference controller, then this is the number of endpoints in active conferences across all managed Telepresence Servers. A Telepresence Server that is not the Conference controller will show zero here. For more information, see Understanding the Conference controller.

Field	Field Description	Usage tips
Video ports	The number of video ports that are being used in any active conferences. The second number is the maximum on this Telepresence Server.	If this is the Conference controller, the numbers are those across all managed Telepresence Servers controlled by this Telepresence Server. SA Telepresence Server that is not the Conference controller will show zero here. For more information, see Understanding the Conference controller and Content channel video support.
Audio ports	The number of audio ports that are being used in any active conferences. The second number is the maximum on this Telepresence Server.	
Content ports	The number of ports that are being used for the content channel in any active conferences. The second number is the maximum on this Telepresence Server.	
System log		
System log	The system log displays the most recent shutdown and upgrade events, with the most recent shown first.	The log will display "unknown" if there has been an unexpected reboot or power failure. If this occurs frequently, report the issues to TANDBERG customer support.
Diagnostic information		
Diagnostic information	Diagnostic information is provided to aid in troubleshooting problems that may occur with the Telepresence Server. In the event of an issue with the Telepresence Server, TANDBERG customer support may ask you for one of these diagnostic files to help with troubleshooting.	Diagnostic files are provided in .zip archive format that contain a text document. To download a diagnostic file, click **Download file**. The network capture file is only available on master blade in a Telepresence Server cluster.
Network capture file		
System logs		

Displaying cluster status for a master blade

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

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

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

The master blade in a cluster inherits all the ports and port licenses from the slaves in the cluster.

Note: Clustering, especially the master blade in a cluster, should not be confused with the Conference controller Telepresence Server. See Understanding clustering.

Field	Field description	Usage tips
Slot	The number of the slot in the MSE chassis to which this row in the table refers.	To configure a blade as a master or a slave in a cluster, go to the web interface of the MSE 8050 Supervisor in the chassis which houses the MSE media blade.
IP	The IP address of the blade in this slot, or *Master blade* (if this is the master).	
Status	The status of the master blade can only be *OK* which means that this blade is operating correctly in the cluster. Possible statuses for a slave blade are: *OK*: The master and slave are communicating correctly. *OK (last seen <number> seconds ago)*: The master has lost contact with the slave. The slave will restart itself and in this way it will rejoin the cluster. Wait a few minutes and then refresh the **Status > Cluster** page. *Still starting up*: The slave blade is in the process of starting up. Wait a few minutes and then refresh the **Status > Cluster** page. *Lost contact <number> secs ago*: The master has lost contact with the slave. The slave will restart itself and in this way it will rejoin the cluster. Wait a few minutes and then refresh the **Status > Cluster** page. *Cluster support not enabled*: There is no Cluster support feature key on this blade. *Failed, version mismatch*: All blades in the cluster must be running the same version of software. This status message indicates that this blade is running different software to the master blade. This blade is not part of the cluster. Update all blades in the cluster to the same version of software.	If the status of the slave is *OK*, it is currently functioning in the cluster. For any of the other statuses, the slave blade is not currently functioning as part of the cluster. If a slave blade has a problem that causes it to no longer be part of the cluster, the cluster can continue to operate without that slave. For example, in a cluster of three blades if one slave fails, the master and the other slave can continue to operate and accept calls. There will just be fewer video ports available. Similarly, in a cluster of two blades, if the slave fails, the master continues to operate. If a slave blade fails, participants in conferences will not be disconnected: if there are sufficient resources on another blade in the cluster, they will continue to receive audio and video. In the worst case, the video will disappear, but the audio will continue because all audio is processed by the master blade. If the master loses contact with a slave, the slave will automatically restart itself. In this way, it can rejoin the cluster.

Field	Field description	Usage tips
	Blade not configured as slave: The Supervisor has told the master that the blade is a slave, but the blade is not a slave. This indicates that someone has removed the slave blade and replaced it with a different blade. *Blade incorrect type*: Someone has removed the blade in this slot and replaced it with a different blade type after the cluster was configured.	
Media processing load	An overview of the current media loading of each blade in the cluster. The load may increase during periods of peak conference use.	Conferences are distributed between the blades in the cluster. The loads on the blades depend on the number of conferences running on each blade and the sizes of those conferences. On a slave blade, the audio load will always be zero: the master is responsible for all the audio.
Port licenses	The number of port licenses on each slot in this cluster.	All port licenses on slave blades are controlled by the master blade. Depending on how you use the blades in the MSE chassis, you might want to allocate all port licenses to the slot that houses the master blade or you might distribute them between the slots in the cluster. It does not matter to the cluster how you have allocated the port licenses; in any case, the master controls all port licenses and even if a blade has failed in the cluster, the master will continue to have access to any port licenses allocated to the failed blade's slot.

Displaying cluster status for a slave blade

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

Cluster status is only available for MSE Media2 blades that are configured on the MSE 8050 Supervisor to be part of a cluster.

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

Slave blades do not display the full MSE Media2 blade web interface. Only certain settings are available.

The master blade in a cluster inherits all the ports and port licenses from a slave blade. To configure conferences and other MCU functionality, you must go to the web interface of the master blade (accessible using the IP address displayed on the **Status > Cluster** page). When you look at the **Status > Cluster** page on a slave blade, it shows the status of the master blade.

Note: Clustering, especially the master blade in a cluster, should not be confused with the Conference controller Telepresence Server. See Understanding clustering.

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

Displaying hardware health status

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

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

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

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

Displaying the conference list

The **Conferences** page lists all the configured conferences on this Telepresence Server regardless of their status (i.e. active, scheduled to occur, or completed). To access this list, go to **Conferences**.

By default, conferences are displayed in alphabetical order. To reorder the list, click on a column heading.

You can:

- Click on a conference to display its status:
  - If this is a configured conference, you can then use additional **Conferences** menu options to edit its configuration
  - If this is a conference started from a room, you are taken to the room's status page.
- Click the  icon next to a conference to display its configuration.
- Click **Add new conference** to set up an additional conference.
- Delete one or more conferences: select them and click **Delete selected**. (You cannot delete a conference started from a room: these conferences are deleted automatically when appropriate.)

The following information is displayed for each conference:

Field	Field description	Usage tips
Name	The name of the conference, which is either the name entered when the conference was set up or the name of the room from which the conference was started.	Click the conference name to display additional information about the conference status and participants. Conferences that have been started from a room have (room) after their name.
Numeric ID registration	The numeric ID assigned to the conference.	Note that, even if a conference has been configured to be registered with the gatekeeper, that registration will not be attempted if the ***Use gatekeeper*** option in **Configuration > System settings** is not selected.
Status	The status of the conference: *Scheduled*, *Enabled*, *Active*, *Inactive* or *Completed*.	Conferences can be: *Active (<X> endpoints) - due to end <time>*: this conference is in progress and has a scheduled end time. *Active - permanent*: this is a permanent conference which has past its start time but may or may not have any active participants. *Inactive*: this conference does not have a scheduled start or end time, nor a numeric ID. It can only be started from the conference's status or configuration pages. *Enabled*: this conference does not have a scheduled start or end time but has a numeric ID, therefore an endpoint can call to the Telepresence server with this numeric ID and start the conference. It will then be shown as *Active (<X> endpoints)* while there are active participants. *Completed*: this conference had a

Field	Field description	Usage tips
		scheduled end time which has passed.

Adding and updating conferences

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

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

Adding a conference

To add a conference:

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

Notes:

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

Updating a conference

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

To update an existing conference:

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

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

   ---

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

Starting an ad hoc conference with pre-configured participants

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

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

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

Field	Field description	Usage tips
Conference		
Name	The name of the conference.	Conference names must be unique.
Numeric ID	The unique identifier used for dialing in to the conference.	Endpoints can join a conference by dialing its numeric ID if the numeric ID and the endpoint are both registered with the gatekeeper. If the conference has a numeric ID that is not registered, you can join the conference by dialing the IP address of the Telepresence Server that is running the conference plus the numeric ID. Conferences do not have to have a numeric ID, but numeric IDs must be unique.
Register numeric ID with H.323 gatekeeper	Whether to register the conference with the Numeric ID as the H.323 ID.	Select this check box to register the conference's numeric ID with the gatekeeper. Endpoints using H.323 can only join this conference by dialing the numeric ID alone if the numeric ID and the endpoint are both registered with the gatekeeper.
Register numeric ID with SIP registrar	Whether to register the conference's Numeric ID with the SIP registrar.	Select this check box to register the conference's numeric ID with the registrar. SIP endpoints can only join this conference by dialing the numeric ID alone if the numeric ID and the endpoint are both registered with the registrar.
Encryption	Whether encryption is optional or required for this conference.	If encryption is *Required*, only endpoints that support encryption can join this conference. Encryption requires a feature key. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server.

Field	Field description	Usage tips
Use OneTable mode when appropriate	Whether to use OneTable mode automatically when the correct combination of endpoints or endpoint groups is in a conference (three or four telepresence endpoints plus less than six other endpoint/endpoint groups). Choose from: *Disabled* *2 person mode* *4 person mode*	In OneTable mode each screen shows an entire view of a single remote site (as opposed to one third of the remote site in a normal, point-to-point telepresence setting). This allows the center four or two participants in three remote telepresence rooms to be seen simultaneously, as if they were seated at one table - depending on whether *4 person mode* or *2 person mode* is selected. For more information, see Understanding how participants display in layout views.
Content channel	If *Enabled*, this conference is able to support an additional video stream, sent potentially to all connected endpoints, intended for showing content video. This content video is typically high resolution, low frame rate data such as a presentation formed of a set of slides. Such presentation data can be sourced by an endpoint specifically contributing a separate content video stream.	For more information, see Content channel video support.
Scheduling		
Schedule	Select the check box to enable the settings in this section.	Conferences can be scheduled using the fields in this section, but you may also want to create a conference without a set start time (in this case, leave this setting unselected). Subsequently, when you want the conference to start, open the conference configuration, add endpoints and click **Start now**.
Start time	The date and time at which the conference will begin.	By default the current date and time are displayed.
Permanent	Allows you to retain a conference and its settings for an infinite period of time.	
End time	The date and time at which the conference will finish.	These fields are not available or necessary for permanent conferences.

Displaying conference status

The **Conference** status page provides details for active conferences. It tells you if the conference:

- is active and how many endpoints are in the conference
- is registered to an H.323 gatekeeper and/or SIP registrar
- includes a content channel
- had previous participants and who they were

To access this page, go to **Conferences**, then select a conference by clicking on its name. The status page of that conference will be displayed by default.

From this page you can:

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

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

The following information is displayed for each conference:

Field	Field description	Usage tips
Status		
Status	The number of endpoints currently in the conference.	Conferences can be: *Active (<X> endpoints) - due to end <time>*: this conference is in progress and has a scheduled end time *Active - permanent*: this is a permanent conference which has past its start time but may or may not have any active participants *Inactive*: this conference does not have a scheduled start or end time, nor a numeric ID. It can only be started from the conference's status or configuration pages *Enabled*: this conference does not have a scheduled start or end time but has a numeric ID, therefore an endpoint can call to the Telepresence server with this numeric ID and start the conference. It will

Field	Field description	Usage tips
		then be shown as *Active (<X> endpoints)* while there are active participants *Completed*: this conference had a scheduled end time which has passed
H.323 gatekeeper status	The status of a conference with respect to its H.323 gatekeeper.	One of: *Numeric ID registered* *Numeric ID failed to register* *Not registered:* conference is not configured to register with the gatekeeper *Registering*: conference is in the process of registering If the Telepresence Server can connect to an H.323 gatekeeper, the name and numeric ID of a conference can be registered with that gatekeeper as a different directory number. This allows H.323 users to dial directly into a particular conference. To configure a H.323 gatekeeper, go to **Configuration > System settings**.
SIP registrar status	The status of a conference with respect to its SIP registrar.	One of: *Numeric ID registered* *Numeric ID failed to register* *Not registered:* conference is not configured to register with the gatekeeper *Registering*: conference is in the process of registering If the Telepresence Server can connect to a SIP registrar, the name and numeric ID of a conference can be registered with that gatekeeper as a different directory number. This allows users to dial directly into a particular conference. To configure a SIP registrar , go to **Configuration > System settings**.
Content	Whether the content channel is being used currently.	One of: *Disabled*: H.239/BFCP content is disabled for the conference. To enable content for this room, go to **Configuration** *No current presentation:* H.239/BFCP content is enabled for the conference but there is no active contributor) *Presentation from <endpoint display name>*: there is an active contributor of H.239/BFCP content For more information, see Content channel video support.
Enter/Leave OneTable mode	Allows you to force the conference's layout in to or out of OneTable mode.	This button is only displayed if ***Use OneTable mode when appropriate*** is disabled for the conference in its

Field	Field description	Usage tips
		Configuration page and there are three or four participants in the conference using multi-screen endpoints.
All participants		
Endpoint	The name of the endpoint currently contributing to 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 **Configuration** page.
Type	The endpoint type.	
Status	The status of the endpoint.	One of: *No endpoints* - the conference has no active participants *Not in a conference* - the endpoint is not active *In conference* - additional status information may be displayed, for example, packet loss is reported If a pre-configured endpoint is busy when the conference starts, the Telepresence Server will retry the endpoint repeatedly throughout the conference and connect it if it becomes free.
More...	Click **More...** to see two previews (of the transmit and receive streams) and be able to control the endpoint's contribution to the conference.	You can: mute  and unmute  audio mute  and unmute  video make a participant important (transmit stream only)  or unimportant 
Previous participants		
Endpoint	The name of the endpoint that was previously in this conference.	
Type	The endpoint type.	
Reason for disconnection	Why the endpoint is no longer part of the conference.	One of: *Requested by admin* *Left conference* *Busy* *Unspecified error*

Understanding how participants display in layout views

Conference layouts

The layout chosen by the Telepresence Server for a system depends on the number of screens that the system has and the characteristics of the other conference participants. The Telepresence Server is capable of working with one-, two-, three- and four-screen regular and Telepresence endpoints, and displaying any combination of those systems participating in a conference to any other type of system in the conference.

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

Layouts sent to one-screen systems

A one-screen endpoint can be configured to receive ***the panel switched view by default*** when possible upon connection, but the layout can be changed using Far End Camera Control.. A one-screen Telepresence endpoint always receives the panel switched view by default when possible. In panel switched view the loudest participant appears full screen with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen.

The panel switched view is possible when the other participants in the conference are all other one-screen endpoints, or a mixture of one-screen endpoints and:

- three-screen Telepresence endpoints that send the details of which screen or panel is sending the loudest audio (the TANDBERG T3 for example).
- grouped three-screen endpoints that send the details of which screen or panel is sending the loudest audio.

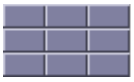
With any other combination of participants, the following rules are applied.

When choosing the layout to show on one-screen systems in a conference, the Telepresence Server takes into account the number of screens used by other participants in the conference.

If there are any four-screen Telepresence systems in a conference, the Telepresence Server sends the following layout to one-screen systems in that conference:

Each row of four panes can either show the four screens of a remote four-screen system or a combination of remote one-, two-, or three-screen systems.

If there are no four-screen Telepresence systems in a conference but there is one or more three-screen systems present, the Telepresence Server sends the following layout to single screen systems in that conference:



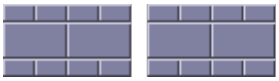
Each row of three panes can either show the three panels of a remote three-screen system or a combination of remote one- and two- screen systems.

If there are only other one-screen and two-screen systems in the conference, the Telepresence Server sends the following layout to one-screen systems:

Each of the two rows of two panes can either show a remote two-screen system or two one-screen systems.

Layouts sent to two-screen systems

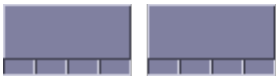
If there are any three- or four-screen Telepresence systems in a conference, the Telepresence Server sends the following layout to two-screen systems in that conference:



Each row of four panes can either show the four screens of a remote four-screen system or a combination of remote one-, two- or three-screen systems.

If there are only other one- and two-screen systems in the conference, the Telepresence Server uses the following layout if all of the video streams to show fit into the available panes:

or the following if a greater number of small panes are needed in order to show more conference participants.



Layouts sent to three-screen systems

If there are any four-screen Telepresence systems in a conference, the Telepresence Server sends the following layout to three-screen systems in that conference:

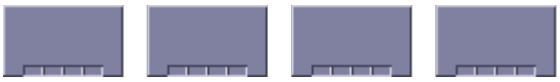
The central row of four large panes can either show the four screens of a remote four-screen system or a combination of one-, two- and three-screen conference participants. In order for this row to be correctly centered, the Telepresence Server shows the panes in the center of the three screens and does 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 the following layouts for three-screen systems in that conference:

Which of these two layouts is chosen depends on the number of other participants in the conference. The layout arrangement with fewer small continuous presence panes will be used if all of the participants to be shown fit within those panes; otherwise the Telepresence Server will use the layout with six small continuous presence panes per screen. The Telepresence Server automatically switches between these two layouts as participants leave and join the conference.

Layout sent to four-screen systems

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



Each row of four panes (the row consisting of the four full-screen panes or one of the rows of four small overlaid panes) can either show a four-screen system or a combination of remote one-, two- and three-screen systems.

OneTable mode

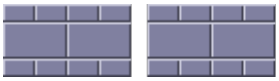
A Telepresence Server in OneTable mode contributes three different video streams of the people in the call, and therefore the Telepresence Server no longer displays the three streams received from these systems side by side in three adjacent panes.

To enable OneTable mode, go to the configuration page of the conference and set ***Use OneTable mode when appropriate*** to *Enabled*. The conference must also have three or more participants present which support the TANDBERG OneTable feature.

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

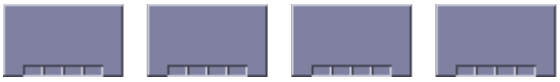
Layout sent to one-screen systems

Layout sent to two-screen systems



Layout sent to three-screen systems

Layout sent to four-screen systems



Configuration options that affect view layouts

This section discusses settings on the Endpoint configuration page that affect view layouts.

Self view setting

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

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

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

to this layout:

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

Show full screen view of single-screen endpoints

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

For single screen systems, the ***Show full screen view of single-screen endpoints*** setting determines whether an endpoint is ever allowed to be shown in a large full-screen pane. If this option is not selected, the endpoint will never be shown full screen to other conference participants, even if it is one of the loudest speakers in the conference. If this option is selected, the endpoint will be shown full screen when it is one of the active speakers in the conference.
(This field is not displayed for multi-screen endpoints and endpoint groups.)

Minimum screen layout setting

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

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

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

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

However, with a setting of *3 screens wide* or *4 screens wide* causes the Telepresence Server to apply the layout choices described above based on the actual number of screens used by the conference participants **and** the virtual presence of a three- or four-screen endpoint. For example, *4 screens wide*

would provide the following layout to all single screen endpoints in the conference even if all of the current participants are using single screen systems.

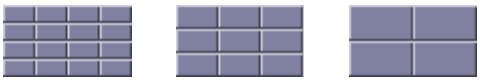
Equally, if you select a setting of *3 screens wide* and a four-screen endpoint joins the conference, the view will change to the one above.

Show continuous presence panes setting

Most multi-screen conference layouts, for example:

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

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



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

Show borders around endpoints setting

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

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

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

Marking a participant as "important"

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

Content channel video support

Most video conferencing endpoints support the use of a second video channel in addition to their main video and audio channels. This second video channel is known as the content channel and is typically used for presentations running alongside live motion video. H.323 video conferencing systems use a protocol called H.239 to receive and send content channel video: BFCP is the SIP equivalent

The content channel is enabled system-wide, but to cater for endpoints that do not support a second video channel, go to **Configuration > System settings** and enable ***Allow content in main video***. When selected, the Telepresence Server will send a conferences' content channel video to endpoints that do not support a separate content video channel in the main video channel sent to those endpoints. In these cases, the content channel video will be shown in place of the normal video — the content channel will replace the normal conference video while the content channel is active (audio is unaffected).

To enable the content channel on a per-conference basis, go to **Conferences > Add new conference**. For ***Content channel***, select *Enabled*.

In each conference, the Telepresence Server allows an active participant to send a content channel video stream, and for that stream to be seen by the other participants in the conference. There can be only one "presenter" in a conference at any time — for a new participant to become the presenter, either the currently active presenter must stop sending content channel video or the Telepresence Server must be configured to allow new participants to take over the presentation from others (see below).

Content channel configuration settings

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

If ***Content channel*** is *Disabled* for a conference, no content channel video is allowed for that conference and no participant in the conference is able to start contributing content channel video. If ***Content channel*** is *Enabled* for a conference, participants are able to contribute content channel video for the other conference participants to see.

For a participant to be able to start contributing a content channel video stream:

- There must either be no other active presenter in the conference or the system-wide ***Automatic content handover*** setting must be *Enabled* in **Configuration > System settings**. If this option is not selected, a participant will not be able to contribute content channel video to the conference while there is another active presenter.
- That participant's endpoint must be configured to allow content channel video contribution. To change whether an endpoint is allowed to contribute a content channel stream, configure its ***Video contribution*** setting to be either *Enabled* or *Disabled* in the **Endpoints > "Endpoint name" > Configuration** page.

For a one-screen participant to be able to see the content channel video, their endpoint must support the H.239 pr BFCP protocol (as appropriate) or the ***Allow content in main video*** setting for their endpoint must be set to *Enabled* in the **Endpoints > Add new endpoint** page.

For a configured endpoint group, the content channel video will be sent to one endpoint in the group, and that endpoint must support the content channel. To choose which endpoint in the group receives the content channel video, use the ***Screen to receive content / audio*** setting for that group in the Advanced settings.

Displaying the endpoint list

The Endpoint list displays all the endpoints that have been configured within the Telepresence Server. This is the list of endpoints from which you can choose when configuring a conference. By default, endpoints are displayed in alphabetical order. To reorder the list, click on a column heading.

To display the Endpoint list, go to **Endpoints**.

From this page you can:

- See an endpoint's status. To do this, click on an endpoint or endpoint group's name
- Add a new endpoint. To do this, click **Add new endpoint**
- Add a new Cisco endpoint. Click **Add Cisco endpoint**.
- Add a new endpoint group. Click **Add grouped endpoints** if available.
  An endpoint group is a group of two or more endpoints that has a name and can be selected as the recipient of a call. These endpoints are then treated as one Telepresence endpoint by the Telepresence Server. A feature key is required to use endpoint groups and therefore the button only displays if the key is installed: feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server.
- Delete configured endpoints. To do this, select the endpoints to delete and click **Delete selected**

Note: Multi-screen endpoints are not grouped endpoints.

Field	Field description
Name	The name of the endpoint.
Type	The type of the endpoint; for example, Standard, TANDBERG Experia or Group of X endpoints.
Status	Whether the endpoint is in a conference, and if it is, the name of the conference.

Adding and configuring endpoints and endpoint groups

You can configure endpoints to use with the Telepresence Server. Pre-configuring endpoints makes it easier to add them to conferences because you can choose names from a list rather than adding network addresses. Endpoints can be single- and multi-screen systems, normal or Telepresence endpoints and devices such as the Codian IP VCR.

A TANDBERG Codian IP VCR can be configured as an endpoint and added as a participant in a conference. If the IP VCR is configured to do so, it will start recording as soon as the conference starts. You can also configure a folder's Recording ID as an endpoint and in this way, when a conference starts, the IP VCR can start recording directly into a specific folder. For more information about using the IP VCR in this way, refer to the IP VCR's online help.

Recordings on a TANDBERG Codian IP VCR can be configured as endpoints. In this way, a participant can contribute an IP VCR recording as his video stream. This function is also useful where you have a recording that you might like to view within a conference.

Adding an endpoint

To add an endpoint:

1. Go to **Endpoints > Add new endpoint**.
2. Complete the fields, using the table in Updating an endpoint or group below for guidance.
   If you want to be able to call out to the endpoint from a conference, you must configure the ***Call-out parameters***.
3. Click **Add new endpoint**.

Adding a Cisco endpoint

To add a Cisco single- or multi-screen endpoint:

1. Go to **Endpoints > Add Cisco endpoint**.
2. Complete the Name and Address.
3. Click **Add Cisco endpoint**. This will take you to the configuration page.
4. Follow the instructions and the table in Updating an endpoint or group below to complete the configuration. (Unless specifically mentioned, fields also apply to a Cisco endpoint.)
   If you want to be able to call out to the endpoint group from a conference, you must configure the ***Call out parameters***. If you want to be able to call out to the endpoint from a conference, you must configure the ***Call-out parameters***.

Adding an endpoint group

You can configure endpoints to work as a group which can then act as a single Telepresence endpoint. To use this function you must have the third party interop feature key installed. (Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server.)

To add an endpoint group:

1. Go to **Endpoints > Add grouped endpoints**.
2. Complete the fields using the table below for guidance.
3. Click **Add grouped endpoints**. This takes you to the configuration page.
4. Follow the instructions in Updating an endpoint or group below to complete the configuration for the endpoints in the group.
   If you want to be able to call out to the endpoint group from a conference, you must configure the ***Call out parameters***.

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

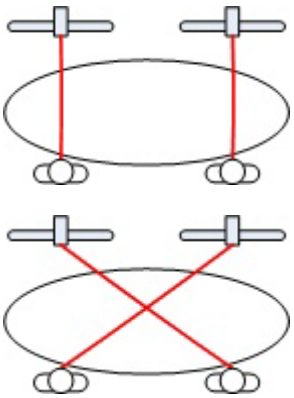
Field	Field description	Usage tips
Name	The name of the group.	
Calling out address list	The list of addresses to call out to when this group is in an active conference.	Enter a list of addresses separated by commas. **Note**: The order must be from left to right in terms of facing the endpoints' screens.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

Updating an endpoint or group

To edit an existing endpoint (including Cisco endpoints) or an endpoint group:

1. Go to **Endpoints**.
2. Click on the name of the endpoint or endpoint group that you want to update.
3. Go to **Configuration**.
4. Update the fields using the table below for guidance.
5. Click **Update endpoint**.
6. If required, go to **Advanced settings** to edit the additional parameters for this endpoint or endpoint group.

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

Field	Field description	Usage tips
Cameras are cross connected	Select this check box for endpoint groups whose outermost camera views cross. This option is only available for endpoint groups.	
Call-out parameters		
Address	The IP address, host name, or an E.164 address (phone number).	For H.323 calls, you can configure this endpoint or endpoint group as needing to be reached via an H.323 gateway. To do this, set this field to be *<gateway address>!<E.164>*.
Call protocol	Select either H.323 or SIP from the drop-down list.	Not applicable to Cisco endpoints which always use SIP.
Use gatekeeper	Select this option to use a gatekeeper when calling this endpoint or endpoint group.	Note that, even if an endpoint or endpoint group has been configured to be registered with the gatekeeper, that registration will not be attempted if the ***Use gatekeeper*** option in **Configuration > System settings** is not selected. This option does not apply to Cisco endpoints because they always use SIP.
Call-in match parameters		
Name	The name that the endpoint or endpoint group sends to the Telepresence Server.	These fields are used to identify incoming calls as being from the endpoint or endpoint group. The endpoint or endpoint group is recognized if all filled-in fields in this section are matched. Fields left blank are not considered in the match. When you configure ***Call-in match parameters***, an endpoint or endpoint group will be recognized as this pre-configured endpoint or endpoint group and the ***Initial status*** parameters will be applied to a call from this endpoint or endpoint group.
Address	The IP address of the endpoint or endpoint group.	
E.164	For H.323 calls, the E.164 address with which the endpoint or endpoint group is registered with the gatekeeper. For SIP calls, the SIP username with which the endpoint or endpoint group is registered with the SIP registrar.	
Initial status		
Audio from	Whether the initial audio from the endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, it will not be able to contribute audio to the conference. For example, you can mute audio from an endpoint or endpoint group if

Field	Field description	Usage tips
		somebody wants to be seen in the conference, but does not want to contribute verbally. You can mute both audio and video if required. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.
Audio to	Whether the initial audio to this endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, the participant using this endpoint or endpoint group will not be able to hear the other participants. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.
Video from	Whether the initial video from this endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, it will not be able to contribute video to the conference. For example, you can mute video from an endpoint or endpoint group if somebody wants to see the conference, but not be seen themselves. You can mute both audio and video if required. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.
Video to	Whether the initial video to the endpoint or endpoint group is either *Active* or *Muted*.	If set to *Muted*, when the endpoint or endpoint group joins a conference, the participant using this endpoint or endpoint group will but not see the other participants, but will be seen themselves. This can be altered during the course of the conference either in the endpoint's or endpoint group's status page, or from the relevant conference's status page.
Display parameters		
Full screen view	This option controls the conditions under which this endpoint will be displayed full screen. This option is only available for single-screen endpoints and does not apply to Cisco endpoints or endpoint groups.	Select a setting from the drop-down list: *Allowed*: This single-screen endpoint will always be allowed to be shown in full screen panes. *Dynamic*: This single-screen endpoint will be allowed to be shown in full screen panes if there are no grouped endpoints to show. However, when there are grouped endpoints to show, the endpoint will then be restricted to the smaller continuous presence panes. *Disabled*: This single-screen endpoint will never be shown in full screen panes. Not displayed for Cisco endpoints.

Field	Field description	Usage tips
Show borders around endpoints	Select this option to show borders around participants displayed in the conference view on this endpoint or endpoint group.	For more information, see Understanding how participants display in layout views.
Active speaker display	Select this option to show a red border around the active speaker on this endpoint or endpoint group.	This setting is only available if *Show borders around endpoints* (detailed above) is selected.
Show endpoint names as panel labels	If you select this option, the Telepresence Server will label view panes in the conference layout sent to this endpoint or endpoint group with the names of the participants shown in those panes.	
Show continuous presence panes	Select this option to allow a mixture of small and large panes in the view sent to this endpoint or endpoint group so that additional participants can be displayed.	For more information, see Understanding how participants display in layout views.
Self view	If this option is not selected, the Telepresence Server will never show the video stream sent from this endpoint or endpoint group to the participants using this endpoint or endpoint group i.e. they will not see themselves.	For more information, see Understanding how participants display in layout views.
Use panel switched view as default	This option controls the default layout that single-screen endpoints see when they connect. Participants can then change their layout using Far End Camera Control. When selected, any single-screen endpoint will use the panel switched view upon connection. In this layout the loudest participant appears full screen with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen	The panel switched view requires that all multi-screen systems in the conference send the Telepresence Server a loudest panel/screen indication. The TANDBERG T3 must be running software version 3.0 or later to send this information. If multi-screen systems that do not send this indication are present within a conference, only the standard single-screen continuous presence view is available. When using the panel switched view the loudest panel/screen of a Telepresence T3 system is displayed full-screen. Not applicable to Cisco endpoints or endpoint groups.
Content		
Video contribution	Whether this endpoint or endpoint group is permitted to contribute content to the conference via content channel.	To use the content channel, the content channel must be enabled for the conference in its configuration page.
Allow content in main video	Whether the Telepresence Server should send content channel video to this endpoint in its main video channel if it is not able to receive a separate video channel. This option is only available for single-screen endpoints and single-screen Cisco endpoints.	This option can be configured to match the Telepresence Server system settings (**Configuration > System settings**) or to be specifically *Enabled* or *Disabled* just for this endpoint.

Configuring endpoints and groups: advanced settings

The Advanced settings page allows you to configure additional parameters for an endpoint, Cisco endpoint or an endpoint group. To do so:

1. Go to **Endpoints** and select the endpoint (including Cisco endpoints) or endpoint group from the list.
2. Go to **Advanced settings**.
3. Complete the fields using the table below for reference.
4. Click **Update endpoint**.

Field	Field description	Usage tips
Video format	The format to be transmitted by the Telepresence Server to this endpoint or endpoint group.	This option should be set to match your endpoint's video configuration. If you set this incorrectly, the smoothness of the video both to and from endpoints might suffer. NTSC is typically used in North America, while PAL is typically used in the UK and Europe. Select a setting from the drop-down list: *PAL - 25fps*: The Telepresence Server will transmit video at 25 frames per second (or a fraction of 25, for example: 12.5fps) *NTSC - 30 fps*: The Telepresence Server will transmit video at 30 frames per second (or a fraction of 30, for example: 15fps) *<use default>*
Transmitted video resolutions	The setting for transmitted video resolutions from the Telepresence Server to this endpoint or endpoint group.	Select a setting from the drop-down list: *4:3 resolutions only* *16:9 resolutions only* *Allow all resolutions* Endpoints advertise the resolutions that they are able to display. The Telepresence Server then chooses the resolution that it will use to transmit video from those advertised resolutions. However, some endpoints do not display widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the Telepresence Server for transmissions to this endpoint or endpoint group.
Motion / sharpness trade off	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint or endpoint group and the Telepresence Server. This setting controls how the Telepresence Server will negotiate the settings to be used.	Select a setting from the drop-down list: *Favor motion*: the Telepresence Server will try and use a high frame rate. That is, the Telepresence Server will strongly favor a resolution of at least 25 frames per second *Favor sharpness*: the Telepresence Server will use the highest resolution that is

Field	Field description	Usage tips
		appropriate for what is being viewed *Balanced*: the Telepresence Server will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)
Default bandwidth (both to and from the endpoint)	The network capacity used by the media channels established by the Telepresence Server to and from this endpoint or endpoint group.	When the Telepresence Server makes a call to an endpoint, it chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio, video, and content channels combined. This setting overwrites the ***Default bandwidth (both to and from the endpoint*** setting in the **Configuration > System settings** page.
Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the Telepresence Server for outgoing video streams (from the Telepresence Server to connected video endpoints).	Typically, you only need to set this value to lower than the default (1400 bytes) if there is a known packet size restriction in the path between the Telepresence Server and potential connected endpoints. Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The Telepresence Server optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size. This setting overwrites the ***Default bandwidth (both to and from the endpoint*** setting in the **Configuration > System settings** page.
Optimization		
<use default>	Selecting this check box overrides any settings in the next three fields and uses the equivalent default conference settings.	The default conference settings are on the **Configuration > System settings** page.
Received video: flow control on video errors	Selecting this check box allows the Telepresence Server to request that the endpoint/endpoint group send lower speed video if it fails to receive all the packets which comprise the far end's video stream.	The Telepresence Server can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased based on the quality of video received by the Telepresence Server. If there is a bandwidth limitation in the path between the endpoint/endpoint group and the Telepresence Server, it is better for the Telepresence Server to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.

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

Displaying endpoint and endpoint group status

You can display the status of endpoints (including Cisco endpoints) and endpoint groups. This shows some general information (for example, the manufacturer) but is most useful when the endpoint is part of an active conference.

To display endpoint and endpoint group status

1. Go to **Endpoints**
2. Click on an endpoint or endpoint group.

The table below explains the information displayed. Click **Refresh** to update the details.

Controlling an endpoint or endpoint group when it is connected

When an endpoint or endpoint group is in an active conference you can use this page to:

- Mute the audio to or from the endpoint or endpoint group
- Mute the video to or from an endpoint or endpoint group
- Disconnect the endpoint or endpoint group

The table below provides more information.

Field	Field description	Usage tips
Endpoint-supplied information		
Country code/extension	These fields display information as returned by the endpoint. The details may not be supplied in a consistent manner between manufacturers.	This information is displayed after the endpoint has been connected for the first time (regardless of whether it's currently connected or not).
Manufacturer code		
Product		
Version		
Status		
Connected to conference	Whether the endpoint is currently in a conference, and if so the name of the conference.	Click the conference name to go to the status page for that conference.
Call status	Whether the call is connected and if so, if it is an incoming or outgoing call.	
Protocol	The protocol used in this call e.g. H.323.	
Endpoint advertised capabilities	The capabilities that the endpoint advertised when negotiating the call.	For example: audio, video, video content, encrypted and unencrypted traffic.
Video channels	Whether receive and transmit video channels are open between the Telepresence Server and the far end.	
Far end audio mute	Whether the audio from the far end has been muted by the remote device.	

Field	Field description	Usage tips
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.
Encryption check code	If encryption is in use for this call, the encryption check code is shown here.	The check code can be used in combination with information displayed by some endpoints to check that the encryption is secure.
Preview	Sample stills of the video stream(s).	The preview shows a still from each screen for both the receive stream (top row) and the transmit stream (bottom row).
Endpoint *X*	The IP address and connection status of each endpoint in an endpoint group.	These fields are only shown for endpoint groups.
Duration	The time that the endpoint/endpoint group has been in this conference.	
Disconnect	Use this control to disconnect the endpoint or endpoint group from the conference.	
Mute audio from / Unmute audio from	Use this control to start or stop muting audio from this endpoint. This changes whether other conference participants will be able to hear this endpoint.	
Mute audio to / Unmute audio to	Use this control to start or stop muting audio to this endpoint. If audio is muted *to* an endpoint, that 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.	"Tidying" a view layout effectively resets and re-centers the participants being shown in that view. This can be useful in a conference after participants have left - the Telepresence Server aims to keep showing people in the same place and so if all participants occupying the center panes disconnect then you can be left with only outside panes being used. Using **Tidy view** in this situation will cause the Telepresence Server to place participants again starting from the center.

Displaying endpoint and endpoint group statistics

You can display the statistics for an endpoint (including Cisco endpoints) or endpoint group.

To do this:

1. Go to **Endpoints**.
2. Click on the endpoint or endpoint group whose statistics you want to see. You are taken to that endpoint's **Status** page.
3. Go to **Statistics**. The information is displayed in three sections: Audio, Video, and Content channel.
4. To update the information shown, click **Refresh**.

The Audio, Video, and Content channel sections are divided into two parts; the Receive stream and Transmit stream.

Field	Field description
Audio/Video/Content channel receive stream	
Encryption	Whether this stream is encrypted.
Channel bit rate	The negotiated available bandwidth for the endpoint to send audio/video/content to the 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 Telepresence Server has requested the endpoint sends. The most-recently measured bit rate displays in parentheses.
Received jitter	Represents the variation in audio/video/content packets when they arrive at the Telepresence Server.
Receive energy	This field applies to the audio receive stream only and is a measure of the level of audio.
Packets received / errors	The number of audio packets that have been received by the Telepresence Server. The second number indicated the audio/video/content packet-level errors, for example, sequence discontinuities, incorrect RTP details, etc. This is not the same as packets in which the video (the actual video data) is somehow in error.
Packets total / missing	The number of audio/video/content packets destined for the 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 and is the number of frames per second being sent to the Telepresence Server from the endpoint.
Fast update requests sent	The number of fast update requests that have been sent to the Telepresence Server.
Audio/Video/Content Transmit stream	
Encryption	Whether this stream is encrypted.

Field	Field description
Channel bit rate	The negotiated available bandwidth for the 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 Telepresence Server is attempting to send at this moment. The actual bit rate, which is simply the measured rate of video data leaving the Telepresence Server, displays in parentheses.
Packets sent	The number of audio/video/content packets destined for the endpoint.
Frame rate	This field applies to the video and content receive streams and is the number of frames per second being sent from the Telepresence Server to the endpoint.
Fast update requests sent	The number of fast update requests that have been sent to the Telepresence Server.

Displaying the Telepresence Server list

The Server list displays all the Telepresence Servers that have been configured to work with this Conference controller Telepresence Server. For more information on the Conference controller, see Understanding the Conference controller.

To display the Server list, go to **Telepresence Servers**. By default, Telepresence Servers are displayed in alphabetical order. To reorder the list, click on a column heading.

On this page you can:

- See a Telepresence Server's configuration and status. To do this, click on a Telepresence Server name.
- Add a new Telepresence Server to be controlled by this Telepresence Server. To do this, click **Add new Telepresence Server**.
- Delete one or more Telepresence Servers. To do this, select the Telepresence Server(s) you want to delete and click **Delete selected**. (The Conference controller Telepresence Server cannot be deleted; therefore its check box is grayed).

Note: Do not confuse the Conference controller feature with a cluster of Telepresence Server. For more information, see Understanding clustering.

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

Adding and updating Telepresence Servers

A Telepresence Server can be configured to be a Conference controller. The Conference controller can control a number of functions on other Telepresence Servers that are configured to be used with it. To configure a Telepresence Server to be a Conference controller, go to **Configuration > System settings**. For ***Conference control***, select *Conference controller - this system will manage all conferences*.

Before a Telepresence Server can be added to the list, its ***Conference control*** setting must be set to *Conferences will be managed by an external controller*.

Note: Do not confuse the Conference controller feature with a cluster of Telepresence Server. For more information, see Understanding clustering.

Adding a Telepresence Server to the Conference controller

1. On the Conference controller Telepresence Server go to **Telepresence Servers > Add new Telepresence Server**.
2. Complete the fields using the table below for guidance.
3. Click **Add new Telepresence Server**.

Updating a Telepresence Server details on the Conference controller

1. On the Conference controller Telepresence Server go to **Telepresence Servers**.
2. Click on the name of the Telepresence Server you want to edit.
3. Change the configuration using the table below for guidance.
4. Click **Update Telepresence Server**.

The status is displayed below the configuration fields and the information shown is explained in the table below.

Field	Field description	Usage tips
Name	The name of the Telepresence Server.	
Address	The IP address of the Telepresence Server.	
HTTP port	The TCP port number on the Telepresence Server which the Conference controller Telepresence Server will attempt to connect to if it is configured to use HTTP for this connection.	This field is only displayed when you add a Telepresence Server.
HTTPS port	The TCP port number on the Telepresence Server which the Conference controller Telepresence Server will attempt to connect to if it is configured to use HTTPS for this connection.	This field is only displayed when you add a Telepresence Server.

Field	Field description	Usage tips
Use HTTPS	When selected, this Telepresence Server will connect to the Conference controller Telepresence Server using HTTPS. HTTPS is a more secure connection than using HTTP.	This field is only displayed when you add a Telepresence Server. If this option is selected, the Telepresence Server will use the ***HTTPS port*** value configured for the Conference controller Telepresence Server, otherwise it will use the ***HTTP port*** value.
Enabled	Whether this Telepresence Server is enabled.	If a Telepresence Server is not enabled, no conferences will be allocated to run on it by the Conference controller.
Telepresence Server status		
Connection status	Whether this Telepresence Server is connected to the Conference controller Telepresence Server.	One of: *Waiting for IP address* *Connecting...* *Connected: Waiting for final phase...* *OK* *Failed to connect to IP address <IP address>. Retrying in <X> seconds* *Connection failed* *Retrying dropped connection in <X> seconds* *Disabled* *Disabled - only conference controllers can manage other systems* *There is a health status problem* *Encryption not supported* *Gatekeeper registration failed*
Licenses	The number of licensed ports.	For more information about licenses, see Understanding screen licenses.
Model	The Telepresence Server model.	
Serial number	The unique serial number of the Telepresence Server.	
Software version	The installed software version. You will need to provide this information when speaking to TANDBERG customer support.	
Build	The build version of installed software. You will need to provide this information when speaking to TANDBERG customer support.	
Fans **Voltages** **RTC battery**	For enabled Telepresence Servers, shows Current status/Worst status seen conditions.	For each of current and worst seen conditions, one of *OK*: component is functioning properly *Out of spec*: check with your support provider; component might require service

Field	Field description	Usage tips
		Critical:: component is in critical condition If the Worst status seen column displays *Out of spec*, but Current status is *OK*, monitor the status regularly to verify that it was only a temporary condition. This field is not displayed for disabled Telepresence Servers.
Temperature	For enabled Telepresence Servers, shows Current status/Worst status seen conditions.	Displays three possible states: *OK*: temperature of the Telepresence Server is within the appropriate range *Out of spec*: Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked <*Critical*: temperature of the Telepresence Server is too high. An error also appears in the event log indicating that the system will shutdown in 60 seconds if the condition persists If the Worst status seen column displays *Out of spec*, but Current status is *OK*, monitor the status regularly to verify that it was only a temporary condition. This field is not displayed for disabled Telepresence Servers.
H.323 gatekeeper status	Whether the Telepresence Server is connected to an H.323 gatekeeper.	If it is, then the gatekeeper's IP address is shown.
Number of active registrations	How many registrations the Telepresence Server has with the gatekeeper.	
SIP boxwide registration status	Whether the Telepresence Server is registered with a SIP registrar.	One of: Registered with Registration in progress SIP registration not enabled No registration configured Failed to register to
Number of active conference registrations	How many conferences the Telepresence Server has registered with the gatekeeper.	
Features	What optional features are active on this slave Telepresence Server e.g. Encryption.	Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server.
Video ports	The number of video ports that are being used in any active conferences. The second number is the maximum number	

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

Understanding the Conference controller

It is possible to set up multiple Telepresence Servers to be controlled by a single Telepresence Server (called the Conference controller). This allows you to use a single set of endpoint, conference and room configurations across multiple Telepresence Servers and monitor them from a single Telepresence Server. However, a conference can only run on one Telepresence Server, limiting the number of participants. This contrasts with a cluster of Telepresence Servers: for more information, see Understanding clustering.

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

Having a Conference controller system has some consequences:

- All calls must be made to the address of the Telepresence Server that is configured to be the Conference controller. This Telepresence Server then decides which Telepresence Server in its system will host each conference. Calls to a Telepresence Server that is not configured to be a Conference controller are not accepted.
- You must log in to the Telepresence Server that is configured as the Conference controller to see status and statistics information.
- If the Conference controller fails, conferences running on a Telepresence Server in its system will continue **until** a new Conference controller is configured. This resets all conferences.
- TANDBERG recommends that you back up the configuration of the Telepresence Server that is configured as the Conference controller so that if you need to change which Telepresence Server acts as Conference controller you can restore endpoint, conference and room information on the new system. See Backing up and restoring the configuration
- Each Telepresence Server has a certain number of screen licenses, and each screen license effectively activates one video port. The Conference controller has use of all the screen licenses for the Telepresence Servers it is working with. For more information about screen licenses, see Understanding screen licenses.

Configuring a single Telepresence Server system

If you are running a single Telepresence Server system, the Telepresence Server must be configured as a Conference controller. To do this, go to **Configuration > System settings**. For ***Conference control***, select *Conference controller - this system will manage all conferences*. This Telepresence Server will now control all calls and conferences.

Configuring a multiple Telepresence Server system

To create a multi-Telepresence Server system, you must configure one Telepresence Server to be the Conference controller and then add Telepresence Servers to it.

To configure the Conference controller:

1. Go to the web interface of the Telepresence Server to be the Conference controller.
2. Go to **Configuration > System settings**.
3. For ***Conference control***, select *Conference controller - this system will manage all conferences*.
4. Click **Apply changes**.

To add additional Telepresence Servers to this Conference controller:

1. Go to the web interface of the Telepresence Server that is now the Conference controller.
2. Go to **Telepresence Servers > Add new Telepresence Server**.
3. Complete the fields. See Adding and configuring Telepresence Servers for more information.

To check communication between the Conference controller and Telepresence Servers configured to work with it, go to **Telepresence Servers**. Ensure that ***Status*** is *OK*.

Understanding clustering

About clustering

Clusters are configured and managed using the Supervisor. A cluster is a group of blades on the same MSE chassis linked together to behave as a single unit that provides the combined screen count of all the blades in the cluster. A larger screen count provides flexibility: either conferences with more participants or several smaller conferences. For more information about screen licenses, see Understanding screen licenses. You can configure two types of cluster:

- **MSE 8510 cluster:** MSE Media2 blades running software version 4.1 or later support clustering.
  Clustering provides you with the combined port count of the blades in the cluster. For example, on an MSE 8510 cluster of three blades each with 20 port licenses, the cluster can have either 30 HD ports or 15 HD+ ports and the master can allocate them to participants in conferences as necessary. This could be one large conference, or several smaller conferences. Note that in a cluster of MSE 8510 blades, SD ports are not available.

  The maximum port counts for clusters comprising three MSE 8510 Media2 blades are as follows:

  - For HD+ mode, the maximum number of port licenses that a three-blade cluster can utilize is 240. This will provide you with a total of 60 HD+ ports.
  - For HD mode, the maximum number of port licenses that a three-blade cluster can utilize is 120. This will provide you with a total of 60 HD ports.

  To configure media ports, on the MCU go to **Settings > Media ports**.

- **Telepresence Server 8710 cluster:** Telepresence Server blades running software version 2 or later support clustering. Currently up to three blades can be clustered, with one blade acting as a "master" and the other blades being "slaves" to this master.
  Clustering provides you with the combined video port count of the blades in the cluster. For example, on an MSE 8710 cluster of three blades each with 16 screen licenses, the cluster has 48 video ports and the master can allocate them to participants in conferences as necessary. This could be one large conference, or several smaller conferences.

Master blades

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

Slave blades

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

General points

Some points to note about clustering:

- To cluster a blade, it requires the cluster support feature key.
- The MSE 8000 Supervisor blade must be running software version 2.1 or above to configure clustering.

- You cannot mix the type of blades in a cluster but you can have both types of cluster in the same MSE chassis.
- All blades in a cluster must be running the same version of software.
- You assign the cluster roles (master/slave) to the slots in the chassis; if a blade fails, you can replace it with a blade of the same type and the cluster configuration will persist; however, what happens to active calls and conferences varies, as described below.
- If you restart or remove the master, the slaves will also restart: all calls and conferences end.
- Blades that do not support clustering can be installed into an MSE chassis alongside a cluster.
- If the clustering configuration on the Supervisor and a blade disagree, then the Supervisor pushes the clustering configuration to the blade. (This might happen if you replace a slave blade with another blade of the same type.) 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.
- Always keep a recent backup of the Supervisor.
- If the Supervisor restarts or is removed, the cluster continues to function, conferences continue, and the cluster does not restart when the Supervisor reappears.
- Slave blades only have admin logins.

Upgrading clustered blades

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

Comparing clustering with the Conference controller Telepresence Server functionality

Do not confuse clustering Telepresence Server blades with the Conference controller:

- Clustering is only possible on MSE 8710 blades, not on 7000 Telepresence Servers. The Conference controller functionality is available in all Telepresence Servers and can be used across MSE 8710 blades and 7000 Telepresence Servers; that is a Conference controller MSE 8710 blade can work with 7000 Telepresence Servers and vice versa.
- Clustering is only available with the Clustering feature key, which must be installed on all the blades that you want to configure as one cluster Telepresence Server. The blades must be in the same MSE 8000 chassis. The Conference controller functionality does not require a feature key.
- Both features allow load balancing and pool screen licenses.
- The master blade in a cluster Telepresence Server controls all the conferences in the cluster, decides which blade a conference will run on, and calls must come in to the master blades. Similarly the Conference controller Telepresence Server controls conferences across all the Telepresence Servers that are configured to work with it, decides which Telepresence Server a conference will run on, and calls must come in to the Conference controller Telepresence Server. However, a cluster allows larger conferences because the processing can be spread over a number of blades. Supposing you have three 8710 blades, each with 10 screen licenses. If they are clustered, then 30 screen licenses are available and the maximum number of participants in a conference is 30. Using the Conference controller: there are still 30 screen licenses but the maximum conference size is 16: the maximum that can run on any one Telepresence Server, even if though there are more screen licenses available.
- The concepts can be mixed: the master blade in a cluster can also be a Conference controller.

Understanding screen licenses

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

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

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

Screen licenses are configured via a screen license key provided by TANDBERG.

- For Telepresence Server 8710 blades housed in an MSE 8000 chassis, the screen license key is configured on the chassis Supervisor blade and then screen licenses allocated to the individual Telepresence Server 8710 blades by an administrator.
- For Telepresence Server devices which operate as standalone units, screen license keys should be entered on the **Configuration > Upgrade** page in the same way as feature keys.

Displaying the rooms list

The Rooms list displays all the rooms that have been configured within the Telepresence Server. By default, rooms are displayed in alphabetical order. To reorder the list, click on a column heading.

To display the Rooms list, go to **Rooms**. (Note that this feature requires the Third party interop feature key. To see which keys are installed go to **Configuration > Upgrade**.)

A room provides a user account for the Telepresence Server. The room is associated with an endpoint (including Cisco endpoints) or endpoint group and a list of pre-configured endpoints. Users who log in to this account can create a conference that includes the associated endpoint or endpoint group and the pre-configured endpoints they require.

From the Rooms list you can:

- See the status of a room. To do this, click on a room name.
- Add a new room. To do this, click **Add new room**.
- Delete one or more rooms. To do this, select the rooms to delete and click **Delete selected**.

The following details are displayed for each room.

Field	Field description
Name	The name of the room.
User ID	The user name to log in to the Telepresence Server with.
Endpoint	The endpoint or endpoint group that is used for this room. Click on an endpoint or endpoint group's name to see its status page.

Adding and configuring rooms

An administrator can create a room to allow a user to create a conference on the Telepresence Server using that room. A room has an endpoint and a user account associated with it, and users who log into this account can create a conference that includes the associated endpoint. The user can also add endpoints (including Cisco endpoints) or endpoint groups that have been pre-configured for use with this account/room.

(Note that this feature requires the Third party interop feature key. To see which keys are installed go to **Configuration > Upgrade**.)

Adding a new room

To add a room:

1. Go to **Rooms > Add new room**.
2. Complete the fields using the table below for help.
3. Click **Add new room**.

You are taken to the configuration page for your new room. This page includes a number of additional fields also explained in the table below.

Updating a room

You can update the configuration of an existing room. To update a room:

1. Go to **Rooms**.
2. Click on the name of the room you want to update from the Rooms list.
3. Edit the fields as required, using the table below for help.
4. Click **Modify room**.

Note: To change the pre-configured endpoints for this room, click **Add pre-configured participants**.

Field	Field description	Usage tips
Name	The name of the room.	
User ID	The ***User ID*** that will be used to log in to the Telepresence Server room.	The user will log in to the Telepresence Server web interface using this User ID and the password (described below).
Password	The ***Password*** that will be used to log in to the Telepresence Server room.	The user will log in to the Telepresence Server web interface using this password. **Note**: When updating a room's configuration, the ***Password*** field is not editable. To change the password, click **Change password**.
Endpoint	The endpoint or endpoint group to be associated with this room.	All configured endpoints and endpoint groups with valid call-out parameters are listed.
Allow call-out to user-supplied address	When selected, the user will be able to enter the H.323 ID or IP address of an endpoint or endpoint group to include in a conference.	This is in addition to selecting other pre-configured endpoints.

Field	Field description	Usage tips
Add all endpoints to conference	When selected, every endpoint configured on the Telepresence Server will be available for the user of this room to select from for their conference.	Selecting this option means that when a user logs in from a room they will always see the most up-to-date list of endpoints and endpoint groups to choose from. If you do not select this option, after the room has been added, you can select which endpoints users of this room will always be able to select from. See Pre-configured participants below.
Conference settings		
Numeric ID	The numeric identifier by which the conferences set up from this room will be known.	Also see ***Register numeric ID with H.323 gatekeeper*** below.
Register numeric ID with H.323 gatekeeper	When selected, the conference is registered with the gatekeeper using the numeric ID as the H.323 ID.	The H.323 gatekeeper is configured on the **Configuration > System settings** page. The room's associated endpoint must be in the conference in order for other endpoints or endpoint groups to be able to join.
Register numeric ID with SIP registrar	When selected, the conference is registered with the gatekeeper using the numeric ID.	The SIP registrar is configured on the **Configuration > System settings** page. The room's associated endpoint must be in the conference in order for other endpoints or endpoint groups to be able to join.
Encryption	Whether encryption is *Optional* or *Required* for conferences started from this room.	If encryption is *Required*, only endpoints and endpoint groups that support encryption can join this conference. Encryption requires a feature key. Feature keys are installed in the **Configuration > Upgrade** page. See Upgrading and backing up the Telepresence Server. Note that in the current release encrypted conferences are not supported for Cisco endpoints.
Use OneTable mode when appropriate	Whether to use OneTable mode. Choose from: *Disabled* *4 person mode* *2 person mode* OneTable mode requires three or more participants which support the TANDBERG OneTable feature.	OneTable mode provides a layout that allows telepresence calls between locations to be represented as though the participants in each location were seated along one side of a table. In OneTable mode each of the three screens in a three-screen Telepresence endpoint, such as TANDBERG's Experia are used to represent one side of the table. For more information, see Understanding how participants display in layout views.
Content channel	If ***Enabled***, this conference is able to support an additional video stream intended for showing content video.	This content video is typically high resolution, low frame rate data such as a presentation formed of a set of slides. Such presentation data can be sourced by: an endpoint specifically contributing a separate content video stream the Telepresence Server being configured

Field	Field description	Usage tips
		to use an endpoint's main video stream as the conference's content channel For more information, see Content channel video support.
Pre-configured participants	Click **Add pre-configured participants**. This will list all endpoints configured on this Telepresence Server. Select the endpoints or endpoint groups to be available to users of this room. When creating a conference, users will only be able to call endpoints or endpoint groups configured for that room.	This list is displayed only after you add a room. If ***Add all endpoints to conference*** is enabled (see above), then all the endpoints currently configured on the Telepresence Server are automatically selected and the list is not available for editing. You can: select individual endpoints to be visible to the room user select all endpoints by selecting the check box in the heading row

Displaying room status

The Room status page provides details for active conferences initiated from that room. It tells you if the conference:

- is active and how many endpoints are in the conference.
- is registered to a gatekeeper.
- includes a content channel.
- had previous participants and who they were.

To access this page, go to Rooms, then select a room. The status page of that room will be displayed by default. (Note that this feature requires the Third party interop feature key. To see which keys are installed go to **Configuration > Upgrade**.)

From this page you can:

- Call one or more endpoints: To do this, select the endpoints from the list and click **Call endpoint**. Alternatively, click **Call endpoint** and enter the IP address, URI, or E.164 number.

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

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

The following information is displayed for each conference:

Field	Field description	Usage tips
Status		
Status	The number of endpoints currently in the conference.	
H.323 gatekeeper status	The status of a conference with respect to its H.323 gatekeeper. One of: *Numeric ID registered* *Numeric ID failed to register* *Not registered:* conference is not configured to register with the gatekeeper *Registering*: conference is in the process of registering	If the Telepresence Server can connect to an H.323 gatekeeper, the numeric ID of a conference can be registered with that gatekeeper as a different directory number. This allows H.323 users to dial directly into a particular conference. To configure a H.323 gatekeeper, go to **Configuration > System settings**.
SIP registrar status	The status of a conference with respect to its SIP registrar. One of: *Numeric ID registered* *Numeric ID failed to register*	To configure a SIP registrar, go to **Configuration > System settings**.

Field	Field description	Usage tips
	Not registered: conference is not configured to register with the gatekeeper *Registering*: conference is in the process of registering	
Content	Whether the content channel is being used currently.	One of: *Disabled*: the content channel is disabled for the conference. To enable the content channel for this room, go to **Configuration** *No current presentation:* the content channel 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 video support.
All participants		
Endpoint	The name of the endpoint currently contributing to the conference.	If the conference is not active, this section shows *No endpoints*. To remove an endpoint from the conference, select the endpoint's corresponding check box and select **Disconnect selected** Click on the endpoint's name to go to its **Configuration** page.
Type	The endpoint type.	
Status	The status of the endpoint.	One of: *In conference* *Joining conference* *No endpoints*: there is no conference running from this room
Previous participants		
Endpoint	The name of the endpoint that was previously in this conference.	If the conference is not active, this section shows *No endpoints*.
Type	The endpoint type.	
Reason for disconnection	Why the endpoint is no longer part of the conference started from this room.	One of: *Requested by admin* *Left conference* *Busy* *Unspecified error* To attempt to reconnect an endpoint, select the corresponding check box and click **Retry connection**.

Logging in from a room

Users can start conferences from a Telepresence endpoint configured for a room. To do this they must have the following information:

- IP address of the Telepresence Server that acts as Conference controller: To find this, go to **Telepresence Servers**).

  Note: Only Conference controllers can connect conferences.

- User name and password to log in to this Conference controller Telepresence Server from their room: To find this, go to **Rooms > "Room name" > Configuration**
- Instructions below - also displayed if they click the icon after they have logged in

Instructions on logging in from a room

1. Open a web browser
2. Type in IP address provided by your system administrator
3. Log in using the user name and password also provided by your system administrator
   All the endpoints you can call are displayed.
4. Select the endpoints for this conference.
5. Click the 

icon.
   The conference starts.
6. To end the conference, click the 

icon.

Note: The conference cannot continue if you leave the conference. However, if endpoints that you selected leave, the conference continues while you are connected. In addition, a system administrator can end a conference at any time using the web interface of the Telepresence Server.

Starting a conference from a room

A room is a user account for the Telepresence Server that is associated with an endpoint (including Cisco endpoints) or endpoint group, and a list of pre-configured endpoints. Users who log in to this account can create a conference that includes the associated endpoint or endpoint group and a selection of the pre-configured endpoints.

For a user to be able to start a conference from a room, you must provide them with the following information:

- The IP address of the Telepresence Server. The IP address can be found on the **Telepresence Servers** page.

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

- The username and password for the room. The username and password can be found on the room configuration page. (Go to **Rooms** and click on the desired room.)

Instructions for users of a room

The following instructions are for users logging into the room and also provide information about starting the conference, as well as in-conference features. Provide these instructions to users who will create conferences from a room.

Logging into the room

1. Open a web browser.
2. Enter the IP address provided by the system administrator.
3. For ***Username***, enter the username provided by the system administrator.
4. For ***Password***, enter the password provided by the system administrator.
5. Click **Log in**.

Starting a conference

The endpoints or endpoint groups that have been pre-configured to be used with this room are displayed. To start a conference and add some or all of these endpoints:

1. Select the endpoints or endpoint groups from the list.
2. If enabled by the system administrator you may be able to enter an address of an endpoint that is not pre-configured. To do this, select the check box and enter the address.
3. Click 

.

The conference now starts and is listed in the **Conferences** page. Conferences started from a room appear in the format <conference name> (room name).

To end this conference, click 

.

Using in conference features

From the room you can:

- Call an endpoint while the conference is in progress. To do this, click the endpoint's 

icon.
- Disconnect an active endpoint. To do this, click the endpoint's 

icon.
- Mute or un-mute an active endpoint’s audio. To do this, click its  and  icons.
- Mute or un-mute an active endpoint’s video. To do this, click its  and  icons.
- Make an active endpoint important. To do this, click the picture of that endpoint.
- Call to an address. To do this, select the check box and enter the address.

Displaying the user list

The **Users** page provides an overview of all configured users on the Telepresence Server and a summary of some of their account settings.

Refer to the table below for assistance.

Field	Field description
User ID	The user name that the user needs to access the web interface of the Telepresence Server. Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.
Name	The full name of the user.
Privilege	Access privileges associated with this user. Either *administrator* or *none*.
User attributes	Displays the access assigned to this user: blank (full access) or *API access*. Administrator users have full access, therefore this field is always blank for them. A user who does not have administrator privileges can be assigned API access. This allows the user to communicate with the Telepresence Server via applications that communicate API commands.

Deleting users

To delete a user, select the user you want to delete and click **Delete selected users**. You cannot delete the admin user.

Adding and updating users

You can add users to and update users on the Telepresence Server. Although most information is identical for both tasks, some fields differ.

Adding a user

To add a user:

1. Go to **Users**.
2. Click **Add new user**.
3. Complete the fields referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Add user**.

Updating a user

To update an existing user:

1. Go to **Users**.
2. Click a User ID.
3. Edit the fields as required referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Modify user** — alternatively, to just change the password, click **Change password**.

Field	Field description	More information

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

Configuring network settings

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

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

IP configuration settings

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

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to *Automatic via DHCP* the Telepresence Server obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to *Manual* the Telepresence Server will use the values that you specify in the Manual configuration fields below.	Click **Renew DHCP** to request a new IP address if you have selected automatic configuration. Port A should never be disabled because it is the primary interface of the Telepresence Server.
Manual configuration		
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify this option if you have chosen *Manual* IP configuration, as described above. For Port A, if the IP configuration setting is set to *Automatic by DHCP* this setting will be ignored.
Subnet mask	The subnet mask required for the IP address you wish to use, for example 255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	
DNS configuration		
Host name	Specifies a name for the Telepresence Server.	Depending on your network configuration, you may be able to use this host name to communicate with the Telepresence Server, without needing to know its IP address.
Name server	The IP address of the name server.	
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first returns that it does not know an address, the

Field	Field description	Usage tips
		secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	This can allow you to use non-fully qualified host names when referring to a device by host name instead of IP address. For example, if the domain name is set to *tandberg.com*, then a request to the name server to look up the IP address of host *endpoint* will actually lookup *endpoint.tandberg.com*.

IP status

Use the IP status fields to verify the current IP settings for the appropriate Ethernet port of the Telepresence Server, which were obtained using DHCP or configured manually (see IP configuration settings) including:

- Host name
- DHCP
- IP address
- Subnet mask
- Default gateway
- Name server
- Secondary name server
- Domain name (DNS suffix)

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the Telepresence Server. Refer to the table for assistance with these settings. When you have finished, click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Specify whether you want this Ethernet port to automatically negotiate its Ethernet settings with the device it is connected to, or if it should use the values that you specify in the Manual configuration fields below.	It is important that your Ethernet settings match those of the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both configured with fixed and matching speed and duplex settings (see below).
Manual configuration		
Speed	Identifies the connection speed: *10 Mbit/s* or *100 Mbit/s*. Use automatic negotiation if a connection speed of *1000 Mbit/s* is required.	The connection speed must match that of the device to which this port is connected. You only need to select this option if you have chosen *Manual* Ethernet settings, as described above.
Duplex	Identifies the connection duplex mode: *Full duplex* Both devices can send data to each other at the same time *Half duplex*	The duplex setting must match that of the device to which this port is connected. You only need to select this option if you have chosen *Manual* Ethernet settings, as described above.

Field	Field description	Usage tips
	Only one device can send to the other at a time	

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether this Ethernet port is connected to or disconnected from the network.	
Speed	The speed (*10*/*100*/*1000 Mbit/s*) of the network connection to the Telepresence Server on this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
Duplex	The duplex mode (*Full duplex* or *Half duplex*) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value cannot be changed and is for information only.
Packets sent	Displays a count of the total number of packets sent from this port by the Telepresence Server. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the Telepresence Server is transmitting packets into the network.
Packets received	Displays a count of the total number of packets received by this port of the Telepresence Server. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the Telepresence Server is receiving packets from the network.
Statistics:	These fields display further statistics for this port. Multicast packets sent Multicast packets received Total bytes sent Total bytes received Receive queue drops Collisions Transmit errors Receive errors	Use these fields for advanced network diagnostics, such as resolution of problems with Ethernet link speed and duplex negotiation.

Configuring IP routes settings

You need to set up one or more routing settings to control how IP traffic flows in and out of the Telepresence Server.

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

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

Port preferences

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

Field	Field description	Usage tips
IPv4 gateway preference	The IP address to which the Telepresence Server will send packets in the absence of more specific routing (see IP routes configuration).	You can only select Port A.
Name server (DNS) preference	The IP address to which the Telepresence Server will send requests to look up unrecognized host names in order to determine their corresponding IP addresses.	You can only select Port A.

IP routes configuration

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

Configuration of routes is divided into two sections: addition of new routes, and the display and removal of existing routes.

Adding a new IP route

To add a new route, enter the details using the table below for reference. Click **Add IP route** to make the addition. If the route already exists, or aliases (overlaps) an existing route, you will be prompted to correct the problem and try again.

Field	Field description	Usage tips
IP address / mask length	Use these fields to define the type of IP addresses to which this route applies. The IP address pattern must be in the dot-separated IPv4 format, while the mask length is chosen in the ***IP address / mask length*** field. The mask field specifies how many bits of the address are fixed; unfixed bits must be set to zero in the address specified.	To route all IP addresses in the range 192.168.4.128 to 192.168.4.255 for example, specify the IP address as 192.168.4.128 and the mask length as 25, to indicate that all but the last seven bits address are fixed.

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 *Gateway* is selected, specify the IP address of the gateway to which you want packets to be directed. Selecting *Port A* results in matching packets being routed to Port A's default gateway (see Configuring network settings).

Viewing and deleting existing IP routes

Configured routes are listed below the **Add IP route** section. For each route, the following details are shown:

- 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 added by the user as described above.

The *default* route is configured automatically in correspondence with the *Default gateway preference* field (see Port preferences) and cannot be deleted. Any packets not covered by manually configured routes will be routed according to this route.

Manually configured routes may be deleted by selecting the appropriate check box and clicking **Delete selected**.

Current IP status

This table shows the current default gateway and name server(s) for Ethernet Ports A and B. No fields can be changed, and are provided for reference when configuring the other parameters described in the sections above.

Configuring IP services

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

Use this page to control the type of services that may be accessed via Ethernet Ports A and B. Refer to the table below for more details.

The Telepresence Server offers IP-based services, such as the web interface and H.323 for making and receiving calls. Depending on the security requirements of your network, it is possible to control which services may be accessed on Ethernet port A, and optionally change the TCP ports they may be accessed on. (Port B is unavailable in the current release of the Telepresence Server.)

To reset all values back to their factory default settings, click **Reset to default** and then click **Apply changes**.

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

Field	Field description	Usage tips
Incoming Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the Telepresence Server using SIP over TLS or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the Telepresence Server. If a port is disabled, this option will be unavailable.
FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	FTP can be used to upload and download Telepresence Server configuration. You should consider disabling FTP access on any port that is outside your organization's firewall. If you require advanced security for the Telepresence Server, disable FTP access. If a port is disabled, this option will be unavailable.
UDP service		
SIP (UDP)	Allow/reject incoming and outgoing calls to the Telepresence Server using SIP over UDP or change the port that is used for this service.	Disabling this option will prevent calls using SIP over UDP. If a port is disabled, this option will be unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B.

Network connectivity testing

The Network connectivity page can be used for troubleshooting issues that arise because of problems in the network between the Telepresence Server and a remote video conferencing device being called (or a device from which a user is attempting to call the Telepresence Server).

The Network connectivity page enables you to attempt to 'ping' another device from the Telepresence Server's web interface and perform a 'traceroute' of the network path to that device. The results show whether or not you have network connectivity between the Telepresence Server and another device. You can see from which port the Telepresence Server will route to that address. For a hostname, the IP address to which it has been resolved will be displayed.

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**.

For each successful 'ping', the time taken for the ICMP echo packet to reach the host and for the reply packet to return to the Telepresence Server is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

For each intermediate host (typically routers) on the route between the Telepresence Server and the remote device, the host's IP address and the time taken to receive a response from that host is shown. Not all devices will respond to the messages sent by the Telepresence Server to analyse the route; routing entries for non-responding devices is shown as <unknown>. Some devices are known to send invalid ICMP response packets (e.g. with invalid ICMP checksums); these responses are not recognized by the Telepresence Server and therefore these hosts' entries are also shown as <unknown>.

Note: The ping message is sent from the Telepresence Server to the IP address of the endpoint that you enter. Therefore, if the Telepresence Server has an IP route to the given IP address, regardless of whether that route lies out of port A or port B, the ping will be successful. This feature allows the Telepresence Server's IP routing configuration to be tested, and it has no security implications.

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

System settings

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

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

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

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

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

Field	Field Description	Tips
Conference control		
Conference control	Choose from: *Conference controller - this system will manage all conferences* *Conferences will be managed by an external controller*	Select an option from the drop-down list. For more information, see Understanding the Conference controller.
H.323 gatekeeper		
Use gatekeeper	Enables the Telepresence Server to use an H.323 gatekeeper for registration of numeric IDs for its conferences.	When disabled then no gatekeeper registrations are attempted (and existing registrations are removed), regardless of other gatekeeper or per-conference settings. When set to enabled registrations with the gatekeeper are attempted, and the gatekeeper is contacted for incoming and outgoing calls. If the gatekeeper does not respond, calls are still connected if possible.
Address	The network address of the gatekeeper to which Telepresence Server registrations should be made.	Can be specified either as a host name or as an IP address. This field will have no effect if ***Use gatekeeper*** (see above) is not selected.
H.323 ID to register	Specifies an identifier that the Telepresence Server can use to register itself with the H.323 gatekeeper.	Before the Telepresence Server can register any IDs with the H.323 gatekeeper, it must make a unit-wide registration. This field is required for the gatekeeper registration. This field has no effect if ***Use gatekeeper*** (see above) is not selected.

Field	Field Description	Tips
SIP registrar		
Use SIP registrar	Enables the Telepresence Server to use a SIP registrar for registration of numeric IDs for its conferences.	When disabled, then no SIP registrations are attempted (and existing registrations are torn down), regardless of other SIP registrar or per-conference settings. When enabled, registrations with the registrar are attempted, and the registrar is contacted for incoming and outgoing calls. If the registrar does not respond, calls are still connected if possible.
Address	Identifies the network address of the SIP registrar.	This field has no effect if ***Use SIP registrar*** (see above) is not selected.
Domain	Identifies the network address of the SIP registrar to which Telepresence Server registrations should be made.	This field has no effect if ***Use SIP registrar*** (see above) is set not selected .
Username	The login name for the Telepresence Server on the SIP registrar.	You need to configure the SIP registrar with details of the devices that will register with it and create a login for each device.
Password	The password for the Telepresence Server on the SIP registrar.	You need to configure the SIP registrar with details of the devices that will register with it and create a login for each device. The password configured on this page needs to match the password in the SIP registrar.
Select SIP transport	Identifies the protocol to be used for call control messages.	If your SIP devices use TCP, select *TCP* as the outgoing transport. If your SIP devices use UDP, select *UDP* as the outgoing transport. If you have the encryption feature key installed and want to encrypt signaling, select *TLS*. The Telepresence Server can accept connections on TCP, UDP and TLS providing those services are enabled on the **Network > Services** page.
Use local certificate for outgoing connections and registrations	Select this option to force the Telepresence Server to present its local certificate when registering with the SIP registrar and when making outgoing TLS calls.	Often, the SIP registrar will not require the local certificate from the Telepresence Server. Only select this option if your environment dictates that the SIP registrar must receive the local certificate.
Conference settings		
Voice switching sensitivity	Determines how easy it is for a participant to replace the active speaker for a conference based on how loudly they are speaking.	A value of 0 means that it is very difficult for the active speaker to be replaced; a value of 100 means the active speaker can be replaced very easily.

Field	Field Description	Tips
Packet loss threshold	Enter the threshold level for packet loss as a percentage. If greater packet loss occurs than this threshold, it will be reported: in the Status page for the conference in the Statistics page for the endpoint whose call is experiencing the packet loss	The most suitable setting will depend on your network and its packet loss characteristics.
ClearVision	When selected, the Telepresence Server will upscale video streams from participants who are sending low resolution video with the purpose of making best use of the Telepresence Server's HD video capabilities.	The Telepresence Server uses intelligent resolution upscaling technology to improve the clarity of low-resolution video.
Automatic content handover	Whether a participant is allowed to interrupt another participant's presentation in a conference by starting one of their own. This is unselected by default.	When selected, if an endpoint attempts to send content when another participant is already sending content, the endpoint would override or cancel any existing presentation.
Indicate presence of audio-only participants	Whether an overlaid icon is shown on video participants' screens to show the presence of audio-only participants in the conference. This is unselected by default.	When selected, a telephone icon is displayed in the top left-hand corner of the screen with a number next to it showing the number of audio-only participants present. For grouped endpoints, the icon is shown on just one of the screens: the middle screen on T3s and Experias for manually-configured groups, on the screen configured as the ***Screen to receive content / audio*** in the group's Advanced settings.
Call out to grouped endpoints if one calls in	If this option is selected, if a call is received from an endpoint which forms part of a manually-configured group the Telepresence Server will call out to the other endpoints in that group.	You should make sure this option is unchecked if the endpoints which make up manually-configured groups are set to call in together - in this case the Telepresence Server will recognise the separate calls and group them automatically.
Display video preview images	When selected, thumbnail preview images of conference participants' video streams are shown on the Telepresence server user interface.	
Default endpoint settings		
Full screen view of single-screen endpoints	This option sets the conditions under which single-screen endpoints are placed in full screen panes of video displays sent to conference participants.	This setting can be overridden by the equivalent Full screen view setting in single-screen endpoints' Configuration page. Select a setting from the drop-down list to be used as the default: *Allowed*: Single-screen endpoints will always be allowed to be shown in full screen panes.

Field	Field Description	Tips
		Dynamic: Single-screen endpoints will be allowed to be shown in full screen panes if there are no grouped endpoints to show. However, when there are grouped endpoints to show, single-screen endpoints will then be restricted to the smaller continuous presence panes. *Disabled*: Single-screen endpoints will never be shown in full screen panes.
Show borders around endpoints	Select this option to show borders around participants displayed in the conference view sent to new endpoints/endpoint groups by default.	For more information, see Understanding how participants display in layout views. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Active speaker display	Select this option to show a red border around the active speaker.	This setting is only available if *Show borders around endpoints* (detailed above) is selected.
Show endpoint names as panel labels	If you select this option, the Telepresence Server will label view panes in the conference layout sent to new endpoints/endpoint groups by default with the names of the participants shown in those panes.	This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Show continuous presence panes	Select this option to allow a mixture of small and large panes in the view sent to new endpoints by default so that additional participants can be displayed.	For more information, see Understanding how participants display in layout views. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Self view	If you unselect this option, the Telepresence Server will never show the video stream sent from this endpoint or endpoint group to the participants using this endpoint or endpoint group by default i.e. they will not see themselves.	For more information, see Understanding how participants display in layout views. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Use panel switched view as default	This option controls the default layout single-screen endpoints see when they connect. Participants can change their layout using Far End Camera Control. When selected, any single-screen endpoint will use the panel switched view upon connection. In this layout the loudest participant appears full screen with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen	The panel switched view requires that all multi-screen systems in the conference send the Telepresence Server a loudest panel/screen indication. The TANDBERG T3 must be running software version 3.0 or later to send this information. If multi-screen systems not supporting this indication are present within a conference only the standard single-screen continuous presence view is available. When using the panel switched view the loudest panel/screen of a Telepresence T3 system is displayed full-screen.

Field	Field Description	Tips
Allow content in main video	If selected, the Telepresence Server will choose to send conferences' content channel video to endpoints that do not support a separate content video channel in the main video channels sent to those endpoints. This means that endpoints which otherwise would not be able to see a conference's content channel video will now be able to do so. In these cases, the content channel video will be shown in place of the normal video — the content channel will replace the normal conference video while the content channel is active (audio is unaffected).	For more information about the content channel, see Content channel video support. This setting can be overridden by the setting in the equivalent field in the endpoint's or endpoint group's Configuration page.
Video format	The format to be transmitted by the Telepresence Server to an endpoint or endpoint group.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. *NTSC* is typically used in North America, while *PAL* is typically used in the UK and Europe. Select a setting from the drop-down list: *PAL - 25fps*: The Telepresence Server will transmit video at 25 frames per second (or a fraction of 25, for example: 12.5fps) *NTSC - 30 fps*: The Telepresence Server will transmit video at 30 frames per second (or a fraction of 30, for example: 15fps)
Transmitted video resolutions	The setting for transmitted video resolutions from the Telepresence Server to an endpoint or endpoint group.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. Select a setting from the drop-down list to be used as the default: *4:3 resolutions only* *16:9 resolutions only* *Allow all resolutions*
Motion/sharpness tradeoff	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between an endpoint or endpoint group and the Telepresence Server. This setting controls how the Telepresence Server will negotiate the settings to be used.	This setting can be overridden by a setting for an individual endpoint or endpoint group in the Advanced settings. Select a setting from the drop-down list to be used as the default: *Favor motion*: the Telepresence Server will try and use a high frame rate. That is, the Telepresence Server will strongly favor a resolution of at least 25 frames per second <*Balanced*: the Telepresence Server will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second) *Favor sharpness*: the Telepresence Server

Field	Field Description	Tips
		will use the highest resolution that is appropriate for what is being viewed
Default bandwidth (both to and from the server)	The network capacity used by the media channels established by the Telepresence Server to unknown endpoints and to new pre-configured endpoints for which a value has not been set.	When the Telepresence Server makes a call to an endpoint, it chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio, video, and content channels combined. For endpoint groups, this is the maximum bandwidth per endpoint. This setting can be overridden for individual endpoints in the Advanced settings page.
Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the Telepresence Server for outgoing video streams (from the Telepresence Server to connected endpoints and endpoint groups).	This setting can be overridden for individual endpoints in the Advanced settings page. Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The Telepresence Server optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size.
Received video: flow control on video errors	Selecting this check box allows the Telepresence Server to request that the endpoint or endpoint group send lower speed video if it fails to receive all the packets which comprise the far end's video stream.	The Telepresence Server can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased based on the quality of video received by the Telepresence Server. If there is a bandwidth limitation in the path between the endpoint/endpoint group and the Telepresence Server, it is better for the Telepresence Server to receive every packet of a lower rate stream than to miss some packets of a higher rate stream. This setting can be overridden by the ***Received video: flow control on video errors*** field in an endpoint's or endpoint group's Advanced configuration page.
Received video: flow control based on viewed size	Selecting this check box allows the Telepresence Server to request that the endpoint or endpoint group send lower speed video if the use of the video from that endpoint does not require as high a speed as the channel allows.	Typically the Telepresence Server would send a flow control message because of this setting if the video from that endpoint was either not being seen at all by other conference participants or if it was being shown only in small layout panes. This setting can be overridden by the ***Received video: flow control based on viewed size*** field in an endpoint's or endpoint group's Advanced configuration page.

Field	Field Description	Tips
Video transmit size optimization	Selecting this check box allows the Telepresence Server to vary the resolution, or resolution and codec, of the video being sent to a remote endpoint within the video channel established to that endpoint.	Select a setting from the drop-down list: *None*: Do not allow video size to be changed during transmission *Dynamic resolution only*: Allow video size to be optimized during transmission *Dynamic codec and resolution*: Allow video size to be optimized during transmission and/or dynamic codec selection With this option enabled, the Telepresence Server can, for instance, decide to send CIF video within a 4CIF channel if this will increase the viewed video quality. The circumstances under which decreasing the video resolution can improve the video quality include: if the original size of the viewed video is smaller than the outgoing channel if the remote endpoint has used flow control commands to reduce the bandwidth of the Telepresence Server video transmission Typically, lowering the resolution means that the Telepresence Server can transmit video at a higher frame-rate. This setting can be overridden by the ***Video transmit size optimization*** field in an endpoint's or endpoint group's Advanced configuration page.
Quality of Service		
Audio/Video	QoS is a term that refers to a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize audio transmissions and video transmissions over HTTP traffic. These settings affect all audio and video packets to H.323 endpoints. All other packets are sent with a QoS of 0.	For more information, see Configuring QoS settings.

Configuring QoS settings

To configure Quality of Service (QoS) on the Telepresence Server for audio and video, go to **Configuration > System settings**. The Quality of Service settings are at the bottom of this page.

QoS is a term that refers to a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize audio transmissions and video transmissions over HTTP traffic. These settings affect all audio and video packets to H.323 endpoints. All other packets are sent with a QoS of 0.

The Telepresence Server allows you to set six bits that can be interpreted by networks as either Type of Service (ToS) or Differentiated Services (DiffServ).

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

To configure the QoS settings you need to enter a six 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

About QoS configuration settings

The table below describes the settings on the **Configuration** page.

Click **Apply changes** after making any changes.

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**.

Displaying and resetting system time

The system date and time for the Telepresence Server can be set manually or using the Network Time Protocol (NTP).

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

System time

The current system date and time is displayed.

If you do not have NTP enabled and need to update the system date and/or time manually, type the new values and click **Change system time**.

NTP

The Telepresence Server supports the NTP protocol. Configure the settings using the table below for help, and then click **Update NTP settings**.

The Telepresence Server re-synchronizes with the NTP server via NTP every hour.

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

If the NTP server is local to Port A or Port B then the Telepresence Server will automatically use the appropriate 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. To configure the default gateway or an IP route, go to **Network > Routes**.

Field	Field description	Usage tips
Enable NTP	If selected, use of the NTP protocol is Enabled on the Telepresence Server.	
UTC offset	The offset of the time zone that you are in from Greenwich Mean Time.	You must update the offset manually when the clocks go backwards or forwards: the Telepresence Server does not adjust for daylight saving automatically.
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)

If NAT is used between the Telepresence Server and the NTP server, with the Telepresence Server on the NAT's local network (and not the NTP server), no extra configuration is required.

If NAT is used between the Telepresence Server and the NTP server, with the NTP server on the NAT's local network, then configure the NAT forwarding table to forward all data to UDP port 123 to the NTP server.

Upgrading and backing up the Telepresence Server

Upgrading the main Telepresence Server software image

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

To upgrade the main Telepresence Server software image:

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

Upgrading the loader software image

Upgrades for the loader software image are not typically available as often as upgrades to the main software image.

To upgrade the loader software image:

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

Backing up and restoring the configuration

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

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, locate a previously-saved "configuration.xml" file and click **Restore backup file**. When restoring a new configuration file to a Telepresence Server you can control which parts of the configuration are overwritten:

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

By default, the overwrite controls are not selected, and therefore the existing network settings and user accounts will be preserved.

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 you should receive the Telepresence Server already activated; if it is not, you have upgraded to a newer firmware version, or you are enabling a new feature, you may need to contact your supplier to obtain an appropriate activation code. Activation codes are unique to a particular Telepresence Server so ensure you know the blade's serial number such that you may receive a code appropriate to your Telepresence Server.

Regardless of whether you are activating the Telepresence Server or enabling an advanced feature, the process is the same. Additionally, if it's a TS 7000 series Telepresence Server, then the port licence key is also entered here.

To activate the Telepresence Server or enable an advanced feature:

1. Check the ***Activated features*** (Telepresence Server activation is shown in this same list) to confirm that the feature you require is not already activated.
2. Enter the new feature code into the ***Activation code*** field exactly as you received it, including any dashes.
3. Click **Update features**. The browser window should refresh and list the newly activated feature, showing the activation code beside it. Activation codes may be time-limited. If this is the case, an expiry date will be displayed, or a warning that the feature has already expired. Expired activation codes remain listed, but the corresponding feature will not be activated. If the activation code is not valid, you will be prompted to re-enter it.
4. TANDBERG recommends that you record the activation code in case you need to re-enter it in the future.

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

Note that you can remove some Telepresence Server feature keys by clicking the **Remove** link next to the feature key in this page.

Shutting down and restarting the Telepresence Server

It is sometimes necessary to shut down the Telepresence Server, generally to restart as part of an upgrade (see Upgrading and backing up the Telepresence Server). You should also shut down the Telepresence Server before intentionally removing power from it.

Shutting down the Telepresence Server will disconnect all active calls.

To shut down the Telepresence Server:

1. Go to **Configuration > Shutdown**.
2. Click the **Shut down Telepresence Server** button.
3. Confirmation of shutdown is required; the button changes to **Confirm Telepresence Server shutdown**.
4. Click again to confirm.
5. 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**.
6. Click this button a final time to restart the Telepresence Server.

Changing the password

This page allows you to change the administrator password used to log in to this Telepresence Server. To access this page, go to **Configuration > Change password.**

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

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

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

Working with the event logs

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

Event log

The last 2000 status messages generated by the Telepresence Server are displayed in 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. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the Telepresence Server, TANDBERG customer support can interpret logged messages and their significance for you.

You can:

- Change the level of detail collected in the traces by editing the **Event capture filter** page. You should not modify these settings unless instructed to do so by TANDBERG customer support.
- Display the log as text: go to **Logs > Event log** and click **Download as text**.
- Change which of the stored Event log entries are displayed by editing the **Event display filter** page.
- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Syslog** page. For more information, refer to Logging using syslog
- Empty the log by clicking **Clear log**.

Event capture filter

The Event capture filter allows you to change the level of detail to collect in the Event log traces.

Note: You should not modify these settings unless instructed to do so by TANDBERG customer support. Modifying these settings can impair the performance of your Telepresence Server.

Normally, the capture filter should be set to the default of *Errors, warnings and information* for all logging sources. There is no advantage in changing the setting of any source without advice from TANDBERG customer support. There is a limited amount of space available to store logged messages and enabling anything other than *Errors, warnings and information* could cause the log to become full quickly.

Event display filter

The Event display filter allows you to view or highlight stored Event log entries. Normally, you should not need to view or modify any of the settings on this page.

Syslog

You can configure the Telepresence Server to send event messages to up to four syslog servers. To add or remove a syslog server, go to **Logs > Syslog** and make the changes you require. See Logging using syslog.

H.323/SIP log

The **H.323/SIP log** page records every H.323 and SIP message received or transmitted from the Telepresence Server. The log can be exported in an .xml file by clicking **Download as XML**.

By default the H.323/SIP log is disabled because it affects performance, but TANDBERG customer support may ask you to enable it if there is a problem with a blade in your network. To do this, click **Enable H323/SIP logging**

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:

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 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 Telepresence Server. **Note:** Various operating system daemons and processes have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar. Various operating systems have been found to 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 these are the values that we recommend you select.

Using syslog

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

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

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

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

Backing up and restoring the configuration using FTP

You can back up and restore the configuration of the Telepresence Server through its web interface. To do so, go to **Configuration > Upgrade**. For more information, refer to Upgrading and backing up the Telepresence Server.

You can also save the configuration of the Telepresence Server using FTP.

To back up the configuration via FTP:

1. On the **Network > Services** page ensure that ***FTP*** is enabled.
2. Connect to the Telepresence Server using an FTP client. When asked for a user name and password, enter the same ones that you use to log in to the Telepresence Server's web interface as an administrator.
   You will see a file called configuration.xml. This contains the complete configuration of your Telepresence Server.
3. Copy this file and store it somewhere safe.

The backup process is now complete.

To restore the configuration using FTP:

1. Locate the copy of the configuration.xml file that you want to restore.
2. On the **Network > Services** page ensure that ***FTP*** is enabled.
3. Connect to the Telepresence Server using an FTP client. When asked for a user name and password, use the same ones that use to log in to the Telepresence Server's web interface as an administrator.
4. Upload your configuration.xml file to the Telepresence Server, overwriting the existing file on the Telepresence Server.

The restore process is now complete.

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

If you are using the configuration file to configure a duplicate blade, for example in a network where you have more than one Telepresence Server, be aware that if the original blade was configured with a static address, you will need to reconfigure the IP address on any other blades on which you have used the configuration file.

Configuring SSL certificates

If the Telepresence Server has the *Secure management (HTTPS)* or *Encryption* feature key installed, and you enable *Secure web* on the **Network > Services** page, you will be able to access the web interface of the Telepresence Server using HTTPS. The Telepresence Server has a local certificate and private key pre-installed and this is used by default when you access the unit using HTTPS. However, we recommend that you upload your own certificate and private key to ensure security because all Telepresence Servers have identical default certificates and keys.

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

If you have uploaded your own certificate and key, you can remove it later if necessary; to do this, click **Delete custom certificate and key**.

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

The table below details the fields you see on the **Network > SSL certificates** page.

Field	Field description	Usage tips
Local certificate		
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 certificate was issued.	
Expires	The date on which the 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 Telepresence Server. The private key is used by the

Field	Field description	Usage tips
		Telepresence Server to decrypt that data. If the ***Private key*** field shows 'Key matches certificate' then the data is securely encrypted in both directions.
Local certificate configuration		
Certificate	If your organization has bought a certificate, or you have your own way of generating certificates, you can upload it. Browse to find the certificate file.	
Private key	Browse to find the private key file that accompanies your certificate.	
Private key encryption password	If your private key is stored in an encrypted format, you must enter the password here so that you can upload the key to the Telepresence Server.	

Contact details and license information

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

TANDBERG

TANDBERG is now part of Cisco. TANDBERG Products UK Ltd is now part of Cisco.

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

Software licenses

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

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

- Info-ZIP
- Independent JPEG Group
- The OpenSSL Project
- AES
- HMAC
- SHA1
- Lua
- DHCP

NetBSD

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

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

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

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

Info-ZIP

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

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

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

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

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

Independent JPEG Group's JPEG software

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

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

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

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

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

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

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

The OpenSSL Project

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

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

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

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

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

Original SSLeay License

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

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

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

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

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

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

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

AES License

LICENSE TERMS

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

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

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

DISCLAIMER

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

Issue Date: 29/07/2002

HMAC License

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

LICENSE TERMS

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

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

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

DISCLAIMER

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

Issue Date: 26/08/2003

SHA1 License

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

LICENSE TERMS

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

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

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

DISCLAIMER

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

Issue Date: 01/08/2005

Lua

Lua 5.0 license

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

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

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DHCP

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

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

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