Cisco TelePresence Server 3.1(1.95)

Software Maintenance Release Notes
October 2013

Contents

Product documentation

Documentation on the installation, configuration, and operation of the TelePresence Server is available on the following sites:

- TelePresence Server installation guides
- TelePresence Server configuration and programming guides
- TelePresence Server administration guides

New platforms for TelePresence Server

Cisco Multiparty Media 310/320

This release introduces new hardware platforms for the TelePresence Server software. These are the same hardware platforms used for the MCU 5300 Series and, similarly, there are two models:

- Cisco Multiparty Media 310
- Cisco Multiparty Media 320

The TelePresence Server software only runs in the remotely managed mode of operation on these new appliances; that is, Cisco TelePresence Conductor XC2.2 (or later), or a similar system, is required to manage the TelePresence Server on these platforms.

Note: Owing to the lack of direct H.323 support in these new platforms, TelePresence Conductor must be configured to run in back-to-back user agent mode (B2BUA mode), or policy server mode with SIP enabled. These platforms cannot be used in an H.323-only TelePresence Conductor deployment.

For the other differences between the TelePresence Server platforms, see Differences between TelePresence Server software on different hardware platforms [p.2].

The TelePresence Server on Media 310 can accept up to 5 screen licenses and the TelePresence Server on Media 320 can accept up to 10 screen licenses. See Platform licensing comparison [p.4] for details of the conferencing capacity associated with these licenses.

A pair of Cisco Multiparty Media 310/320 appliances can be clustered (or 'stacked') to increase conferencing capacity. You can cluster a Media 310 with a Media 320 (a 'mixed cluster'), but **you cannot cluster more than two of these appliances**. You will need to procure an MCU 5300 Series stacking cable to cluster your Media 310/320 appliances (the same cable is used for both types of appliance).

Running TelePresence Server software on MCU hardware

You can replace the MCU software with TelePresence Server software on the following MCU hardware platforms:

- MCU MSE 8510 (blade)
- MCU 5300 Series (appliance)

We do not support the 'reverse' feature — that is, replacing the TelePresence Server software with MCU software — on any hardware platforms.

You can cluster the hardware after you replace the software, using the procedures documented in the software replacement guides (see links below). There is also an option to use your existing MCU conferencing capacity (media port licenses) to provide conferencing capacity for the TelePresence Server (screen licenses) after you replace the software.

Refer to the following MCU documentation sites for detailed instructions on how to replace the software on your MCU with TelePresence Server software:

- Cisco TelePresence MCU MSE Series install and upgrade documentation
- Cisco TelePresence MCU 5300 Series install and upgrade documentation

Differences between TelePresence Server software on different hardware platforms

The following table indicates the differences between the TelePresence Server software when it is running on different hardware platforms. Most TelePresence Server features have the same level of support across all platforms, so the table only shows the relevant subset of the available features.

The table does not list the feature differences between locally managed and remotely managed modes of operation, as locally managed mode is only available on the 7010 and MSE 8710 platforms. Refer to the

release notes for TelePresence Server version 3.0, and the associated administrator documentation, for more details.

Table 1: Differences between TelePresence Server platforms

Feature name	TelePresence Server on		
	7010	MSE 8710 or MCU MSE 8510	Media 310/320 or MCU 5300 Series
Remotely managed mode	Yes	Yes	Yes*
Locally managed mode	Yes	Yes	No*
SIP support	Yes	Yes	Yes
H.323 support	Yes	Yes	Not directly. Requires H.323 ↔ SIP interworking by Cisco VCS.
FTP	Yes	Yes	No
Clustering	No	Yes‡	Yes‡
G.723.1	Yes	Yes	No
Interlaced H.263 support	Yes	Yes	No
Isolated media processor reboots	No	No	Yes, on Media 320 or MCU 5320, or TelePresence Server clusters on these platforms
Replacing MCU software with TelePresence Server software	No	Yes, on MCU MSE 8510	Yes, on MCU 5300 Series
Maximum screen licenses per unit	12	12†	5 on Media 310, or MCU 5310† 10 on Media 320, or MCU 5320†

* Remotely managed mode is the only mode of operation of the TelePresence Server on these platforms, hence they have no concept of the difference between these modes and there is no mention of operation mode in the user interface.

‡ Running identical software on the units in a cluster is an absolute requirement for clustering but mixed hardware is possible to a limited extent. For example, an MCU MSE 8510 running TelePresence Server software can be clustered with a TelePresence Server MSE 8710, provided they have identical TelePresence Server software versions. Similarly, a TelePresence Server on Media 310 can be clustered with TelePresence Server running on an MCU 5320.

† When TelePresence Server software is running on MCU hardware, it is possible to allocate screen licenses to the application but TelePresence Server screen licenses are not interchangeable with MCU media port licenses. See the software replacement documentation for more details, including how to use MCU capacity to provide capacity for the TelePresence Server application.

Platform licensing comparison

The following table compares the number of TelePresence Server screen licenses that each of the platforms can accept and how they translate into conferencing capacity. The table does not display information about licensing for the locally managed mode of operation, as this is only possible on the 7010 and MSE 8710 platforms. Refer to the online help or administrator documentation for details of licensing in locally managed mode.

Note: The numbers in the corresponding table in the online help for the TelePresence Server may not correspond with those shown here. The table shown here takes precedence over the help.

Table 2: TelePresence Server conferencing capacity on various platforms

Call type description			**Screen licenses required per call**	**Maximum calls by hardware type (with licenses to provide 100% of capacity)**						
Main video	**Audio**	**Content**		**10-core VM**	**Media 310 or MCU 5310**	**Media 320 or MCU 5320**	**7010**	**MSE 8710 or MCU MSE 8510**	**Biggest appliance cluster (two appliances)**	**Biggest blade cluster (four blades)**
				6 screen licenses	**5 screen licenses**	**10 screen licenses**	**12 screen licenses**	**12 screen licenses**	**20 screen licenses**	**48 screen licenses**
-	Mono	-	1/52	104*	104*	104*	104*	104*	104*	104*
360p30†	Mono	In main video	⅛	49	41	81	97	97	104*	104*
480p30	Mono	In main video	¼	24	20	40	48	48	80	104*
480p30	Stereo	720p5	⅓	18	15	30	36	36	60	104*
720p30	Stereo	720p5	½	12	10	20	24	24	40	96
720p30	Stereo	720p30	1	6	5	10	12	12	20	48
1080p30	Stereo	720p15	1	6	5	10	12	12	20	48
720p60	Stereo	720p15	1	6	5	10	12	12	20	48
1080p30	Stereo	720p30	1 ½	4	3	6	8	8	13	32

Call type description			Screen licenses required per call	Maximum calls by hardware type (with licenses to provide 100% of capacity)						
Main video	**Audio**	**Content**		**10-core VM**	**Media 310 or MCU 5310**	**Media 320 or MCU 5320**	**7010**	**MSE 8710 or MCU MSE 8510**	**Biggest appliance cluster (two appliances)**	**Biggest blade cluster (four blades)**
				6 screen licenses	**5 screen licenses**	**10 screen licenses**	**12 screen licenses**	**12 screen licenses**	**20 screen licenses**	**48 screen licenses**
Three-screen‡ 720p30	Multichannel	720p5	1½	4	3	6	8	8	13	32
Three-screen‡ 720p30	Multichannel	720p30	2	3	2	5	6	6	10	24
1080p30	Stereo	1080p30	2	3	2	5	6	6	10	24
Dual-screen‡ 1080p30	Stereo	720p30	2	3	2	5	6	6	10	24
Three-screen‡ 1080p	Multichannel	720p30	3	2	1	3	4	4	6	16
Three-screen‡ 1080p	Multichannel	1080p30	4	1	1	2	3	3	5	12
Four-screen‡ 1080p	Stereo	1080p30	4	1	1	2	3	3	5	12

* 104 is the maximum number of calls that is possible on a TelePresence Server.

‡ The TelePresence Server needs the *Third Party Interop* feature key to host conferences with multi-screen endpoints that are not third party interoperable. This includes all multi-screen endpoints except the Cisco TelePresence System T3 and TIP-compatible endpoints.

† Requires TelePresence Conductor XC2.2 or later.

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

New features in 3.1

ActiveControl to endpoints

ActiveControl is a new feature of the TelePresence Server that improves the conference experience for participants in conferences hosted on TelePresence Servers. The feature is used on a per call basis when the TelePresence Server is remotely managed. There are no web interface settings for ActiveControl and it does not require any configuration.

Notes:

- This feature is only available in the remotely managed mode of TelePresence Server operation. It is not available in the locally managed mode.
- The iX protocol that enables ActiveControl is disabled by default because it is not recognized by some older systems, including Cisco Unified Communications Manager versions earlier than 9.0. You can enable the protocol on a per call basis, using the API, but be aware that this may have unpredictable consequences, including call failure, if there are such older systems in the call path.
  If you wish to use the ActiveControl feature with Cisco Unified CM, then we recommend that you connect your TelePresence Server to a Cisco Unified CM running version 9.1.2 or later (although versions 9.0 and 9.1 also recognize iX). You should also disable the iX Channel on trunks between that Cisco Unified CM and others that are running pre- 9.0 versions (uncheck **Allow iX Application Media** checkbox in the Trunk Specific Configuration section of the SIP Profile Configuration window).
  Refer to the *Optimized Conferencing for Cisco Unified CM and Cisco VCS Release 2.0 Solution Release Notes*, at http://www.cisco.com/en/US/products/ps11775/prod_release_notes_list.html, for more details on enabling iX within your Optimized Conferencing deployment.
- ActiveControl cannot currently traverse firewalls.

The features enabled by ActiveControl require corresponding support in the endpoints' software and user interfaces to maximize their potential. This feature is supported on endpoints that are running TC version 6.2

software, provided that the endpoints have Touch controllers. The following endpoints are capable of running TC 6.2; follow the links to the user guides to read about the interface options that use ActiveControl.

- Cisco TelePresence System Quick Set Series (C20, SX20) User guides for Quick Set Series
- Cisco TelePresence MX Series (MX200, MX300) User guides for MX Series
- Cisco TelePresence System EX Series (EX60, EX90) User guides for EX Series
- Cisco TelePresence Profile Series (Profile 42", 52", 52" Dual, 65", and 65" Dual) User guides for Profile Series
- Cisco TelePresence Integrator C Series (Codecs C40, C60, and C90) User guides for C Series

ActiveControl provides a mechanism for the TelePresence Server to report conference information, so that the endpoints can display this information to the user. Participants can use their endpoints to change properties of the conference. Access to these controls can be granted based on the participant's role:

- By default, guests have control over their own endpoints
- By default, chairpersons have control over the conference and the endpoints of other participants

Some of the available controls are local, in that they affect the participant's own endpoint, including:

- Changing the local layout (more details below)
- Disconnecting the endpoint from the conference

Authorized participants can also disconnect other participants.

Participant list

The TelePresence Server creates a participant list containing the display names of all connected participants, and distributes this list to all endpoints that can accept it. The participant list includes active video participants, those who are on hold or connecting, and audio-only participants, but it does not show disconnected participants. The participant list displayed to the user indicates who is currently the active speaker.

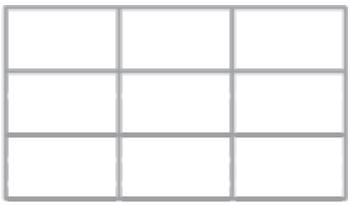
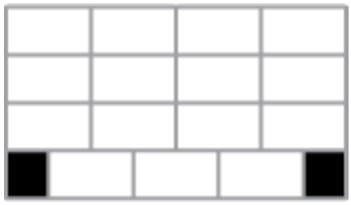
Conference layout

Endpoints that support ActiveControl can control the layout they receive from the TelePresence Server in a number of ways. The TelePresence Server listens for commands from the endpoint that select:

- Which of the TelePresence Server's layouts the participant wishes to see.
  Multiple-screen endpoints can select either ActivePresence or single screen layouts, while single-screen endpoints have those two options as well as prominent and equal layouts. See Table 3: TelePresence Server layout families [p.8] or the online help for more details on layout families.
- Whether the participant wants to see content in the main video display.

ActiveControl does not replace DTMF control for endpoints that can negotiate ActiveControl; you can still use DTMF to control the layout and camera, as with previous versions of TelePresence Server software.

Table 3: TelePresence Server layout families

Name and description	Example layouts
Overlay layouts show the active speaker or content and up to nine overlaid continuous presence panes (per screen) showing other recently active speakers. These are called *ActivePresence* layouts on the TelePresence Server.	
Single screen layouts only show the active speaker or content. On multi-screen endpoints, other recent speakers will show on the additional screens.	
Prominent layouts show the active speaker or content and up to four of the most recent loudest speakers. This is the default layout used if the endpoint chooses to show content in main video. This layout is not available on multi-screen endpoints.	
Equal layouts show a grid of up to 4, 9, or 16 of the most recent active speakers in equal panes, depending on the number and type of endpoints in the conference. Multi-screen endpoints are displayed together in a horizontal group and may be centered if the grid is wider than the number of screens in the endpoint. This layout is not available on multi-screen endpoints.	  

PSTN audio support for WebEx Enabled TelePresence meetings

This release adds support for PSTN audio WebEx meetings where previously the TelePresence Server (version 3.0) required SIP for the audio portion of the WebEx call. You can read more about WebEx Enabled TelePresence with TelePresence Server 3.0 at http://www.cisco.com/en/US/docs/telepresence/infrastructure/tms/config_guide/webex_enabled_telepresence/cts_webex_bridge.html.

Customers can now choose to use SIP or the PSTN for the audio portion of the call between WebEx and the TelePresence Server. This feature only applies to the call between WebEx and the TelePresence Server, and does not affect the audio connections between WebEx participants and the WebEx conference (which can be PSTN audio, SIP audio, or computer telephony).

This feature requires that the *Third Party Interop* key is loaded on the TelePresence Server. The TelePresence Server must be part of a Webex Enabled TelePresence deployment. See the *Cisco WebEx Enabled TelePresence Configuration Guide*, at http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html, for details.

Conference experience improvements

Smaller video formats

This release improves the conference experience for participants whose connections are not adequate for larger format video. Such participants may now be able to conduct video conversations where previously their experience may have been limited to audio-only.

The TelePresence Server can now send 90p and 180p video formats. These formats are 160 by 90 and 320 by 180 respectively. Prior to this release, the TelePresence Server could accept these resolutions but would not send them.

The API can also be used to force the layout sent to particular participants, ensuring that those participants who view the conference at smaller resolutions need not receive a composed layout, which would be less useful to them than a fullscreen view.

Defered connection and auto disconnect

In this release you can pre-configure endpoints for defered connection, which means that the TelePresence Server does not invite those endpoints until at least one other participant is in the conference. You can also pre-configure endpoints to disconnect automatically if there are no other endpoints in the conference.

These two options complement the auto reconnect feature of pre-configured endpoints. The auto reconnect feature has been extended to allow the TelePresence Server to always reconnect, even after the endpoint has deliberately disconnected.

CAUTION: Do not use the **Always reconnect** feature with a user endpoint because the TelePresence Server will repeatedly redial that endpoint, even when the participant deliberately disconnects the call. This feature is designed for automatically connecting integrated systems.

Improved conference status icons

The TelePresence Server has improved icons for conference status, as follows:

Table 4: Improved conference status icons

New overlay	Meaning
	The conference is being recorded
	The conference is unsecured / unencrypted
	The conference has audio-only participants (the number of audio-only participants appears on the right of the handset symbol)

The TelePresence Server overlays these icons, when appropriate, over the video streams composed and sent to endpoints. If ActiveControl is enabled, the TelePresence Server sends the icon state information to endpoints so that endpoints can use their own indications (where supported).

Improved mute behavior

In previous releases, muting an endpoint from the TelePresence Server side would cause the endpoint to be removed from the list of previous loudest speakers, and that participant's video could disappear suddenly from the layout.

In this release, the behavior has been improved so that muting an endpoint from the TelePresence Server's web interface, or via ActiveControl, behaves in the same way as if the participant had muted the endpoint. The endpoint remains in the previous loudest speakers list and the video does not suddenly disappear from the layout.

Suppress audio during DTMF

The TelePresence Server now suppresses the audio coming from an endpoint when the TelePresence Server is sending the connection DTMF sequence to the endpoint, so that other participants do not hear the audio from the endpoint while it is connecting.

The audio suppression continues until the whole DTMF sequence is complete, even if the sequence contains leading or trailing commas - which create pauses of two seconds each.

This suppression is independent of other audio muting options and also persists during retries. This is necessary in combination with the persistence feature because, if the TelePresence Server needs to redial an endpoint in the middle of the conference, the other participants should not hear the audio from the endpoint while it is connecting.

Note: the maximum length of the DTMF sequence has been extended to 127 characters. In prior versions there was a 31 character limit.

Improved room switching

This release improves the way that TelePresence Server displays video from systems with multiple cameras, screens, and microphones ("multi-screen endpoints", for shorthand) to other conference participants using multi-screen endpoints.

The TelePresence Server can now use streams from a multi-screen endpoint to fill large panes that would otherwise be left blank if someone using that endpoint was not the loudest speaker.

For example, consider a conference in which all participants are using three-screen endpoints except for two who are using single-screen endpoints. In the previous releases, when one of the participants using a single-screen endpoint was the active speaker, the TelePresence Server would send the feeds from the two single-screen endpoints to all the three-screen endpoints, and would fill the third screen of those endpoints with a blank / empty feed.

In the same scenario, this release of the TelePresence Server uses a feed from one of the other multi-screen endpoints in place of that blank pane, to make sure that all the endpoint's screens are used.

Content support up to FullHD on Immersive Cisco TelePresence endpoints

The TelePresence Server can now support content streams of up to Full HD resolution to and from TIP-capable endpoints.

Calls between the TelePresence Server and the following endpoints can include a content channel up to 1080p30:

- Cisco TelePresence System 500-32 (with TX 6.0 software)
- Cisco TelePresence TX1300 Series, TX9000 Series, TX9200 Series (with TX 6.0 software)

1080p30 content in a TelePresence Server conference with these endpoints is possible provided that the calls have adequate media resources and that the content source is 1080p30.

The upper limits of the TelePresence Server's content capabilities are described in the following table.

Table 5: TelePresence Server content channel upper limits

Operation mode	Frame resolution	Frame rate
Remotely managed	1920 x 1080 (Full HD)	30 fps
Remotely managed	1280 x 720 (HD)	60 fps
Remotely managed	1920 x 1200 (WUXGA)	27 fps
Locally managed	1280 x 720	5 fps (with TelePresence Server in HD mode)
Locally managed	1280 x 720	15 fps (with TelePresence Server in FullHD mode)

Cisco ClearPath support

The TelePresence Server now supports ClearPath to improve media resilience within lossy networks.This feature is always enabled for all TelePresence Server platforms and does not require any configuration.

The TelePresence Server implementation of ClearPath includes FEC (Forward Error Correction) and two other techniques which are only used inside the video streams, namely LTRF (Long Term Reference Frames) and incoming GDR (Gradual Decoder Refreshes).

ClearPath will be negotiated with any endpoints that support ClearPath, and the TelePresence Server's web interface and API will report statistics on the media resilience techniques used in those calls.

The following endpoints currently support ClearPath in their most recent software releases:

- Cisco Jabber Video for TelePresence
- Cisco Jabber
- Cisco TelePresence System T Series
- Cisco TelePresence System Quick Set Series (C20, SX20)
- Cisco TelePresence MX Series (MX200, MX300)
- Cisco TelePresence System EX Series (EX60, EX90)
- Cisco TelePresence Profile Series (Profile 42", 52", 52" Dual, 65", and 65" Dual)
- Cisco TelePresence Integrator C Series (Codecs C40, C60, and C90)

FEC (Forward Error Correction)

The TelePresence Server applies FEC to enable media packet recovery on outgoing video, audio, and content streams. It can also process incoming streams containing FEC packets and will try to recover media packets lost from these streams.

The technique involves interleaving the original stream with additional, corrective packets, so that if media packets are lost they can potentially be recovered by the recipient without resorting to retransmission of the originals.

Applying FEC consumes additional bandwidth, so a call negotiated at a certain maximum bandwidth will use less bandwidth for the media streams because it needs overhead for the FEC packets. The bandwidth overhead can range from 0% - which means that FEC packets are not used - to 100% when every media packet is protected by a FEC packet. A 50% overhead means that one corrective packet is inserted to protect every two media packets.

The TelePresence Server only starts using FEC when it observes packet loss and then dynamically adjusts the overhead based on the monitored packet loss.

Improved resource efficiency at 360p

Note: This feature is only available in the remotely managed mode of TelePresence Server operation. It is not available in the locally managed mode.

This feature requires version XC2.2 of Cisco TelePresence Conductor.

The TelePresence Server now supports 360p30 video calls more efficiently than it did in previous releases. The TelePresence Server now requires only an eighth of a screen license to support a 360p30 video call with mono audio, where previously a call like this consumed a quarter of a screen license.

This optimization means that the Cisco TelePresence Server 8710, for example, can support up to 97 calls at 360p30 where previously the maximum was 48. See Platform licensing comparison [p.4] for more details.

Automatic Gain Control (AGC)

You can now apply automatic gain control (AGC) to conferences or to individual participants in advance so that the gain is automatically controlled when participants have different audio levels.

AGC adjusts the participants' audio levels to a common reference level to ensure a consistent audio experience for all participants.

A participant's AGC setting always overrides a setting inherited from the conference settings. Automatic gain will be disabled for a connected participant when you manually change the gain.

Serviceability improvements

This release introduces several improvements to the serviceability of TelePresence Servers, as follows:

Protocols log

The protocols log now includes a capture filter, allowing you to capture only those protocols that are relevant to your troubleshooting process.

You can select from the following protocols: BFCP, H.323 (where supported), SIP, and XCCP. H.323 is not directly supported by TelePresence Server on Media 310/320 platforms.

The protocol capture options that you select will persist in the event of a device restart.

Media resources software resilience

A TelePresence Server's media resources are the processor chips that provide its audio and video processing capabilities.The software that controls these processors has been improved in this release to

make it more robust to corrupt or invalid incoming bitstreams.

Isolated media processor reboot

The TelePresence Server on Media 320 is now more resilient in the unusual circumstances of individual media processor failure. On Media 320 models, or mixed Media 310/320 clusters, if a media processor fails it will not cause the whole device to fail. This means that the other parts of the device software can maintain the state of the conferences—except for the tasks performed by that particular processor—while recovering the processor gracefully.

Note: Some participants may experience a loss of video in the unlikely event of a media processor failure, although it should come back after a pause of about 30 seconds.

In the case of a processor failure, the TelePresence Server isolates the processor as well as it can, while rebooting the processor, as follows:

- The TelePresence Server tries to reallocate tasks from the failed processor to other media resources if available. Participants may see a glitch while the tasks are recovered.
- If there are no spare media resources available, the affected participants will experience a loss of video but the calls will stay up while the affected processor reboots.
- The processor reboots in about 30 seconds and video to the affected participants will resume.

Improved diagnostic logging

This release features increased diagnostic detail, particularly in the core system and media processing software, which is continuously monitored and, in the event of a failure, stored for troubleshooting purposes. After a failure, the diagnostic log can be retrieved via the web interface.

The new diagnostics include:

- Improved Cisco TAC diagnostic options in the event of system failures.
- Deeper detail about the TelePresence Server - model and serial numbers, software version, and last reboot reason.
- Information about each media processor, including the state of the active decoders and encoders at the time of failure.
- Information about the endpoint associated with each decoder, and the participant display name.

API message log

This release introduces API message logging to the TelePresence Server. All inbound API messages are recorded in a circular buffer that is written out to a file when the log is requested.

Additional logging options

This release introduces an option to disable the output of event log messages to the TelePresence Server's serial console. This output has been disabled by default to improve performance.

While disabled, the event log messages are still output to the serial console during startup; from the time the TelePresence Server powers up until the media resources are available. After that time, no event log messages are output to the serial console, even though other system messages will occasionally be output.

You can re-enable serial output of event log messages on the **Configuration > System settings** page, but we recommend that you refrain from doing so unless it is under the guidance of the Cisco Technical

Assistance Center. If your deployment relies on this serial console output for troubleshooting, we recommend that you configure a syslog server to capture event messages from the TelePresence Server.

Disconnection of inactive calls

The TelePresence Server now responds to inactive calls by disconnecting them. If media is expected from an endpoint but is not received for 30 to 45 seconds, then the TelePresence Server will disconnect the call. When media has unexpectedly stopped in this way, the TelePresence Server will not show a frozen frame from that stream; it will show no video until it disconnects the call (this aspect of the feature addresses issue number CSCub64800).

This feature applies to any calls using H.323, SIP, or TIP call protocols. If auto-reconnect is enabled for the call, the TelePresence Server retries the call after disconnecting it.

The TelePresence Server will not disconnect a call if the endpoint has signaled that it is on hold or if the media channels are muted.

Resolved issues

The following issues were found in previous releases and are resolved in 3.1(1.95).

Resolved since version 3.1(1.80)

Identifier	Description
CSCuj88766	In some circumstances, negotiation that involves an unusually high number of SIP media lines can cause the TelePresence Server to restart.
CSCuj54065	An error message such as the following may appear on a Cisco Multiparty Media 310/320 running 3.1(1.80): **`HEALTH_MONITOR Error sensor CC0 T0 core failed: reading 1127.000000 mV should be between 980 and 1120 mV`**. In 3.1(1.80), these messages may not be indicative of a genuine problem. An upgrade to version 3.1(1.95) is advised so that genuine voltage problems are not masked by spurious error messages.
CSCuj31071	Modifying a connected pre-configured endpoint using the participant.set API command, on a locally managed TelePresence Server API, could result in an erroneous fault: "Fault 5: 'no such participant'" and an event log message "attempt to set attribute overrides for call with configured endpoint". This is now resolved.
CSCuj05358	Lipsync issues could be observed when endpoints connected at lower bandwidths (< 1Mbps), with packet loss, and the TelePresence Server applied Forward Error Correction to the video channel. This issue was observed on TelePresence Server MSE 8710 and TelePresence Server 7010 platforms. This is now resolved.
CSCui45750	Minor video quality issues were observed on 1080p30 calls on TX9000 series endpoints. These issues included frame skips, background mottling, and blurring during high motion (eg. walking across the camera field of view). This has been improved in this release.
CSCuh35020	The online help pages highlighting the differences between different platforms did not have equivalent detail for Cisco TelePresence Server on Virtual Machine. This is now resolved.

Identifier	Description
CSCui91240	Upon being merged into a TelePresence Server conference by an EX90 endpoint, a Cisco Unified IP Phone 9971 did not display any video. This is now resolved.
CSCui77823	In a specific deployment model, where a Session Border Controller and Cisco TelePresence Exchange System were used, holding and resuming a call from a TC series endpoint would cause the BFCP-based presentation sharing to fail. This is now resolved.
CSCuj04249	The TelePresence Server would occasionally restart when trying to automatically reconnect an endpoint to a conference in which a presentation was being shared. This is now resolved.
CSCui55633	The TelePresence Server would incorrectly timestamp some ClearPath messages to endpoints. This occasionally resulted in loss of video from some older, ClearPath-enabled, endpoint software. This is now resolved.
CSCui45636	When placing a call to the WebEx grouped endpoint, while TMS was configured to "Limit Ports to Number of Scheduled Participants", the TelePresence Server would not be able to complete the TSP audio leg of the call, owing to insufficient video resources. This is now resolved.
CSCui10757	The TelePresence Server would unnecessarily change the outgoing resolution when a three-screen system disconnected. This is now resolved.
CSCui24964	Entering Ctrl+C at the serial console would disable media processor monitoring on the Media 310/320 platforms. This issue did not affect normal operation, but it meant that diagnostic data would have been unavailable in the unlikely event of a media processor failure. This is now resolved.
CSCui85663	The TelePresence Server would not send content to an endpoint if that endpoint had advertized encryption for all channels other than the content channel. This is now resolved.

Resolved since version 3.0(2.48)

Identifier	Description
CSCug48899	In certain previous releases, it was not possible to send overlaid messages on muted video streams. This is now resolved.
CSCue98303	In certain previous releases, the TelePresence Server would fail to dial out to pre-configured endpoints if the TelePresence Server did not have a SIP username configured. This is now resolved.
CSCub64800	A feature has been added to ensure that the TelePresence Server detects when an endpoint fails to send any media for a fixed period and will disconnect the call.
CSCub48355	DTMF tone suppression was not supported in previous versions of TelePresence Server. This is resolved by a new feature in this release.

Identifier	Description
CSCug37686	In previous releases, an endpoint advertising that it will send but not receive video was incorrectly reduced to an audio-only call. This is now resolved.
CSCub87160	In previous releases, the call security status reported on a TIP-capable endpoint could differ from the security status reported in a TelePresence Server conference. This is now resolved.

Open issues

The following issues apply to this version of Cisco TelePresence Server.

Identifier	Description
CSCuh58152	The TelePresence Server does not support ClearPath for the source content channel from ClearPath-enabled endpoints.
CSCuf03190, CSCuf07863	In some circumstances, 1080p video to a Cisco TelePresence System endpoint may show some artifacts. The issue is more likely to occur when using a mixture of 1080p and lower resolution endpoints in a conference. The video artifacts occur less frequently at 1080p if the endpoint is running software version 1.10, and do not occur if the TelePresence Server is sending 720p to the endpoint. This issue has been observed on Cisco TelePresence System 500-37, Cisco TelePresence 1000, Cisco TelePresence 1100, Cisco TelePresence System 1300 65, and Cisco TelePresence System 3000 Series endpoints.
CSCuh24586	The TelePresence Server fails to detect loss of media from an endpoint that loses its connection while it has no active video decoders. This can happen when the affected endpoint is in a large conference (if the TelePresence Server is not showing the stream from that particular endpoint to anybody else) or when the affected endpoint is at the lobby screen, waiting to join the conference. The result is that the TelePresence Server cannot automatically disconnect the affected call.
CSCuh51452	The TelePresence Server sometimes incorrectly processes 1920 x 1200 content at 27fps, sending it out as 1920 x 1080 at 30fps instead.

Limitations

Video issues with earlier versions of TX endpoint software

Note: We strongly recommend that you use TX6.0.5 on these endpoints when they interoperate with TelePresence Server 3.1(1.95).

The following endpoints display significant orange or green flashes when they are using software versions between TX6.0.0 and TX6.0.4 in calls with TelePresence Server 3.1(1.95):

- Cisco TelePresence System 500-32
- Cisco TelePresence TX1300 Series
- Cisco TelePresence TX9000 Series
- Cisco TelePresence TX9200 Series

Resource optimization causes brief video interruptions

When TelePresence Conductor optimizes the resources used for a call, that endpoint's video contribution is very briefly interrupted. This can be visible to others as a flicker of black in the otherwise continuous stream. Issue identifier CSCuj53830.

Call transfer is disabled

The TelePresence Server does not support call transfer.

DTLS and custom certificates

DTLS is used to negotiate encryption parameters with TIP endpoints. This requires a certificate to be used. There are some limitations when using DTLS with customer-supplied certificates:

- Opportunistic DTLS, as supported in release 2.2, always uses the default certificate for DTLS negotiation, even if a customer-supplied certificate is uploaded. This is due to technical limitations.
- Release 2.3 and later supports a new improved DTLS type — 'negotiated DTLS'. When using 'negotiated DTLS', the TelePresence Server uses the customer-supplied certificate if they have uploaded one (which is the preferred procedure). If 'negotiated DTLS' is used in a call to a CTS endpoint combined with some custom certificates, DTLS may fail on these calls. This is due to defect CSCts24503. The call may still connect but without encryption. As a workaround, use a smaller custom certificate such as a certificate with a 1024 byte key or use the default certificate on the TelePresence Server.

HD quality indicators on CTS endpoints

The lobby screen is a static image that is designed for HD mode, that is, 720 pixels high. When a CTS endpoint displays the lobby screen, it may go on to incorrectly report the quality of the received video stream. The quality indicator may show four bars – for 720p video – even though the endpoint is actually receiving 1080p video and should display five bars.

Encryption required causes issues with some endpoints

Some endpoints such as the Sony XG-80 and HG-90, and the TANDBERG Classic 6000s are unable to join conferences in which encryption is required, even when encryption is enabled on the endpoint. (TANDBERG is now part of Cisco.)

Setting these conferences to have optional encryption allows these endpoints to join using encryption.

Clustering limitations

Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering in this TelePresence Server software release. However, slot 10 in the same chassis as a cluster can be used for a standalone blade of any type.

Calls from Microsoft Lync which do not use Advanced Media Gateway may fail

For direct calls from Microsoft Lync or OCS you must use the VCS B2BUA. Calls may no longer work if configured through a VCS zone with profile "Microsoft Office Communication Server". For more information on configuring the VCS, refer to the VCS Administrator documentation.

Firefox 14 is not supported for use with the Cisco TelePresence Server

We strongly recommend that you do not use Firefox 14 to access the TelePresence Server's web interface. This version of the browser causes an issue that was not present in previous Firefox versions and has been fixed in Firefox 15. This issue also affected previous versions of the TelePresence Server software.

TIP calls and encryption required conferences

TIP calls can only join conferences with the Encryption setting configured to *Required* when TLS encrypted signaling is used throughout the call signaling path. This ensures that the call is fully secure.

Recommended VCS version X7.2 or later

On calls to CTS endpoints in certain network configurations, calls may fail or become audio-only with earlier versions of VCS. In order to avoid this, upgrade VCS to X7.2. If using a custom zone profile on VCS for the Cisco Unified Communications Manager zone, ensure that **SIP UPDATE strip** mode is disabled on this zone.

Interoperability

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

We endeavor to make our Cisco TelePresence products interoperable with all relevant standards-based equipment. Although it is not possible to test all scenarios, the testing on which this data is based covers most common functions of the listed endpoints and infrastructure.

About the interoperability section

The interoperability section describes the equipment and software revisions that were tested for interoperability with TelePresence Server 3.1. The absence of a device or revision from this section does not imply a lack of interoperability.

Interoperability testing often requires interworking from one signaling/call control protocol to another. The following table lists phrases that are used to briefly describe the call paths that were tested for each interoperability scenario. The explicit call paths in the table place the endpoint first and the TelePresence Server last as a general convention. References to 'TS' mean either TelePresence Server behind Cisco TelePresence Conductor or TelePresence Server on its own.

Call path phrase	Explicit call path description
SIP	Endpoint ← SIP → TelePresence Server
H.323	Endpoint ← H.323 → TelePresence Server
H.323 to SIP interworking	Endpoint ← H.323 → Cisco VCS ← SIP → TelePresence Server
SIP to H.323 interworking	Endpoint ← SIP → Cisco VCS ← H.323 → TelePresence Server
CUCM to VCS H.323 interworking	Endpoint ← SIP → Cisco Unified CM ← SIP → Cisco VCS ← H.323 → TelePresence Server
CUCM to VCS/Conductor SIP	Endpoint ← SIP → Cisco Unified CM ← SIP → Cisco VCS/TelePresence Conductor ← SIP → TelePresence Server

Call path phrase	Explicit call path description
TIP	Endpoint ← SIP → Cisco Unified CM ← SIP → Cisco VCS/TelePresence Conductor ← SIP → TelePresence Server with TIP negotiation (requires compatible endpoint)

Endpoints

This section lists interoperability issues with endpoints. Where an endpoint has limitations, such as a lack of support for encryption or content, the interoperability tests omitted the limitations and they are not listed here.

An infrastructure issue may manifest itself as an issue with a particular endpoint or series of endpoints; issues of this nature are listed separately under 'Infrastructure'.

Cisco TelePresence

Endpoint	Software	Comments
Cisco IP Video Phone E20	TE4.1.2.299752	Tested H.323 and SIP: ■ Using hold/resume functionality on a Cisco IP Video Phone E20 stops the endpoint from receiving content from the Cisco TelePresence MCU or Cisco TelePresence Server. The endpoint receives content in the main video. (Issue identifier CSCty98376)
Cisco Jabber for iPad	9.2	Tested SIP and SIP to H.323 interworking: ■ Transition from video to content or content to video may lead to transient video issues. (Issue identifier: CSCud64312) ■ Video may occasionally fail when a call that is experiencing packet loss and has FEC protection enabled is optimized from 1080p down to 720p. Pressing the multifunction sleep/wake/on/off button and then pressing it again may work around this issue
Cisco Jabber for Windows	9.2.1	Tested CUCM to VCS/Conductor SIP and CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended
Cisco Jabber Video for TelePresence (Mac OSX)	4.6(17194)	Tested SIP and SIP to H.323 interworking: ■ Video to and from this endpoint can have incorrect aspect ratio when using H.263 or H.263+ (these are not the default codecs)
Cisco Jabber Video for TelePresence (Movi)	4.6.3.17194	Tested SIP and SIP to H.323 interworking: ■ In some cases increasing resources for a call will result in low frame rate from the endpoint. (Issue identifier CSCud79739)

Endpoint	Software	Comments
Cisco TelePresence Codec C40	TC6.1.1	Tested H.323 and SIP: ■ No issues found
Cisco TelePresence Content Server	S5.3	Tested H.323 and SIP: ■ In low bandwidth H.323 calls, an incorrect aspect ratio may be chosen ■ Changing the display settings during the call may cause streaming and podcast output to fail ■ DTMF is not supported in Conductor-based deployments
Cisco TelePresence SX20 Quick Set	TC6.1.1	Tested H.323, SIP, CUCM to VCS/Conductor SIP, and CUCM to VCS H.323 interworking: ■ No issues found
Cisco TelePresence System 500-37	1.10.1	Tested TIP: ■ Under rare circumstances video artefacts may be seen when leaving the lobby screen in 720p calls. (Issue identifier CSCuh92519) ■ Calls can connect at the wrong bandwidth when SIP UPDATE messages are disabled in the call path, for example, when the call is routed via Conductor. (Issue identifier CSCuh97074) ■ If the conference security state changes to insecure, and then changes back to secure, the security indicator on this endpoint still (incorrectly) indicates that the conference is insecure ■ You cannot disconnect audio add-in participants via the participant list on the touch panel. (Issue identifier CSCuj50089) Tested CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended

Endpoint	Software	Comments
Cisco TelePresence System 1700 MXP	F9.3.1	Tested H.323 and SIP: ■ Automatic content handover does not work if MXP tries to present immediately after another endpoint sends content. (Issue identifier CSCud64503) ■ Under rare circumstances, corruption may be seen when the MXP transmits content in main video. (Issue identifier CSCuh93850) ■ Under some circumstances, continuous presence panes are cropped off the bottom of the screen when this endpoint is receiving CIF/4CIF resolutions. (Issue identifier CSCuh93846) ■ High motion video to the MXP 1700 can result in repeated transient corruption. This issue is only seen with Media 310/320 platforms, and when the resolution sent to the endpoint is w576p or above
Cisco TelePresence System 3000	1.10.1	Tested TIP: ■ Video corruption is occasionally visible on this endpoint after a resolution change in the stream from the TelePresence Server. (Issue identifier CSCui10757) ■ Calls can connect at the wrong bandwidth when SIP UPDATE messages are disabled in the call path. For example, when routed via Conductor, a 4MB per screen call connects at 4MB total, leaving about 1.17 MB per screen for video. (Issue identifier CSCuh97074) ■ If the conference security state changes to insecure, and then changes back to secure, the security indicator on this endpoint still (incorrectly) indicates that the conference is insecure ■ You cannot disconnect audio add-in participants via the participant list on the touch panel. (Issue identifier CSCuj50089) Tested CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended
Cisco TelePresence System EX60	TC6.1.1	Tested H.323 and SIP: ■ A flicker is seen when the video from a participant changes from a continuous presence pane into the main pane. Seen when active speaker changes or when making a participant important. (Issue identifier CSCuh92611)

Endpoint	Software	Comments
Cisco TelePresence System EX90	TC6.1.1	Tested H.323, SIP, and CUCM to VCS/Conductor SIP: ■ A flicker is seen when the video from a participant changes from a continuous presence pane into the main pane. Seen when active speaker changes or when making a participant important. (Issue identifier CSCuh92611) Tested CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended
Cisco TelePresence C Series, Cisco TelePresence System EX Series	TC6.2	Tested SIP: ■ These endpoints occasionally exhibit high latency and video corruption in low bandwidth calls. (Issue identifier CSCui40418)
Cisco TelePresence C Series, Cisco TelePresence MX Series, Cisco TelePresence SX20 Quick Set, Cisco TelePresence System EX Series	TC5.1.7	Tested SIP: ■ The endpoint does not respond to normal keyframe requests when it receives incorrect timestamps in ClearPath messages. The issue can manifest as a loss of video from the endpoint. (Issue identifier CSCui34688) This issue can be worked around by disabling ClearPath on the endpoint. The issue is resolved by upgrading the endpoint software.
Cisco TelePresence System TX1300 47, Cisco TelePresence System TX9000	TX6.0.2	Tested TIP: ■ Orange or green flashes can be seen on the display of these endpoints in 1080p30/720p60 calls. (Issue identifier CSCui78297) ■ In some circumstances, content video sent to the TX1300 47 may show artefacts ■ If the conference security state changes to insecure, and then changes back to secure, the security indicator on this endpoint still (incorrectly) indicates that the conference is insecure ■ You cannot disconnect audio add-in participants via the participant list on the touch panel. (Issue identifier CSCuj50089) Tested CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended We recommend that you use TX software 6.0.5, or later, with TelePresence Server software 3.1 (1.95).

Endpoint	Software	Comments
Cisco TelePresence System TX1300 47, Cisco TelePresence System TX9000	TX6.0.3	Tested TIP: ■ Orange or green flashes can be seen on the display of these endpoints in 1080p30/720p60 calls. (Issue identifier CSCui78297) ■ You cannot disconnect audio add-in participants via the participant list on the touch panel. (Issue identifier CSCuj50089) Tested CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended We recommend that you use TX software 6.0.5, or later, with TelePresence Server software 3.1 (1.95).
Cisco TelePresence System TX1300 Series, Cisco TelePresence System TX9000 Series	TX6.0.5	Tested TIP: ■ You cannot disconnect audio add-in participants via the participant list on the touch panel. (Issue identifier CSCuj50089) Tested CUCM to VCS H.323 interworking: ■ Interworking calls from this endpoint is not recommended
T3 TelePresence, T1 TelePresence	TC6.0.1	Tested version TC6.0.1/TCU4.2.1 in remotely managed mode. Tested H.323: ■ PIN entry and layout changing will not function as the T1 and T3 do not support DTMF/ FECC to theTelePresence Server ■ Note that some T1 and T3 functionality is not supported when the TS operates in Remotely Managed mode ■ T3 systems will prefer 1600x1200 resolution when XGAp60 should be shown Tested H.323 to SIP interworking: ■ No issues found

Cisco

Endpoint	Software	Comments
Cisco Desktop Collaboration Experience DX650	10-0-1-110	Tested CUCM to VCS/Conductor SIP and CUCM to VCS H.323 interworking: ■ No issues found
Cisco Unified IP Phone 9971	9.3.2 SR1	Tested CUCM to VCS/Conductor SIP and CUCM to VCS H.323 interworking: ■ Video calls connect as audio-only if call bandwidth is below 280 kbps

Huawei

Endpoint	Software	Comments
ViewPoint 9039	VCT V100R011C02B013SP40	Tested H.323 and SIP: ■ Although this endpoint is interoperable in certain scenarios, it is not recommended with prefered Cisco TelePresence deployments

LifeSize

Endpoint	Software	Comments
Express 220	4.11.13	Tested H.323 and SIP: ■ Although this endpoint is interoperable in certain scenarios, it is not recommended with prefered Cisco TelePresence deployments
Icon 600	LS_RM3_ 1.1.1 (7)	Tested SIP: ■ Although this endpoint is interoperable in certain scenarios, it is not recommended with prefered Cisco TelePresence deployments

Microsoft

Endpoint	Software	Comments
Lync 2010 (without AMGW)	4.0.7577.4103	Tested SIP and SIP to H.323 interworking: ■ This endpoint may display incorrect aspect ratio during low bandwidth calls ■ Hold/resume works incorrectly if initiated while the TS is sending a reINVITE ■ DTMF fails after the TS sends a reINVITE
Microsoft Lync 2010 through Cisco TelePresence Advanced Media Gateway	4.0.7	Tested SIP and SIP to H.323 interworking. Tested with AMGW 10.1(1.34): ■ This endpoint may display incorrect aspect ratio during low bandwidth calls ■ Under rare circumstances, the unencrypted icon can display when the call is encrypted ■ In some circumstances, optimization may not result in an increase in video quality, but will not adversely affect call quality

Polycom

Endpoint	Software	Comments
HDX 8000	3.1.1.3-36019	Tested H.323 and SIP: ■ HDX does not support redial missed/rejected calls due to an endpoint limitation ■ If the endpoint and TelePresence Server are registered to different peers of a VCS cluster, call bandwidth may be limited to 64 kbps. This issue only occurs with H.323 calls ■ Media quality may be unreliable when using H.261 or H.263 (these are not the default codecs). Use the default codec to avoid this issue
HDX 9006	3.1.0-23277	Tested H.323 and SIP: ■ HDX does not support redial missed/rejected calls due to an endpoint limitation ■ If the endpoint and TelePresence Server are registered to different peers of a VCS cluster, call bandwidth may be limited to 64 kbps. This issue only occurs with H.323 calls ■ Media quality may be unreliable when using H.261 or H.263 (these are not the default codecs). Use the default codec to avoid this issue
OTX 300	3.1.0-23277	Tested H.323 and TIP: ■ OTX does not support redial missed/rejected calls due to an endpoint limitation ■ If the endpoint and TelePresence Server are registered to different peers of a VCS cluster, call bandwidth may be limited to 64 kbps. This issue only occurs with H.323 calls ■ 4:3 content sent to OTX may be displayed as 16:9 due to endpoint limitation ■ Encryption is not supported in TIP call architecture ■ DTMF tones are not suppressed
RealPresence Group 500	4.0.2-40451	Tested H.323 and SIP: ■ Siren14 and H.263 codecs are not supported due to endpoint limitations. ■ Low bandwidth H.323 calls do not support encryption ■ FECC does not work over SIP when the call is via CUCM ■ Endpoint may continue to use higher bandwidth after optimization ■ SIP calls to this endpoint may fail if TIP support is enabled on the endpoint. Work around this issue by adding it as a legacy TIP endpoint on the TelePresence Server (if in locally managed mode), or using the "force TIP" option via the API (if in remotely managed mode)

RadVision

Endpoint	Software	Comments
Radvision XT5000	3.0	Tested H.323 and SIP: ■ 60fps video is not supported in calls with this endpoint ■ The TelePresence Server only supports H.264 to this endpoint (default codec) ■ Encryption and the G.722.1 audio codec are not supported in SIP calls ■ We recommend disabling HiP/TSVC on this endpoint, when using it with the TelePresence Server, because it can cause video to fail during calls ■ 1080p content is not supported due to an endpoint limitation

Sony

Endpoint	Software	Comments
PCS-G50	2.72	Tested H.323 and H.323 to SIP interworking: ■ At low bandwidths, in H.323 to SIP interworked calls, this endpoint may not handle audio properly. You can mitigate this by disabling AAC codec for this endpoint ■ Video to this endpoint may fail if the TelePresence Server is in remotely managed mode, because the default aspect ratio in that mode is 16:9. Work around this issue by setting the TelePresence Server to allow all resolutions.

Infrastructure

Endpoint	Software	Comments
Cisco TelePresence Conductor	XC2.2	No issues found.
Cisco TelePresence Video Communication Server (VCS)	X7.2.2	■ Ensure that the "SIP SDP attribute line limit mode" is set to "Off" on zones used by TelePresence Server calls if they are configured with a custom zone profile ■ Increasing resources for a call that leaves the TelePresence Server as H.323 and is interworked by the VCS to SIP can cause the call to fail. (Issue identifier CSCud64471)

Endpoint	Software	Comments
Cisco Unified Communications Manager	8.6.2.21900-5	If the iX protocol is enabled on the TelePresence Server (for ActiveControl), then calls will fail. To work around this, either disable iX on the TelePresence Server or route calls through a newer version of Unifed CM with iX disabled on the relevant trunk.
Cisco Unified Communications Manager	9.0.1.10000-37	If the iX protocol is enabled on the TelePresence Server (for ActiveControl), then call hold may fail. (Issue identifier CSCug89748)
Cisco Unified Communications Manager	9.1.1.10000-11	If the iX protocol is enabled on the TelePresence Server (for ActiveControl), then call hold may fail. (Issue identifier CSCug89748)
Cisco Unified Communications Manager	9.1.2	No issues found.

Upgrading to 3.1(1.95)

Prerequisites and software dependencies

Software dependencies

In the case of the TelePresence Server MSE 8710 blade(s), the Cisco TelePresence Supervisor MSE 8050 blade must be running Supervisor software version 2.2 or later.

Prerequisites

The software upgrade process requires a hardware restart. Schedule a downtime window and notify users of when the service will be unavailable. The duration of an upgrade can be up to 25 minutes. Have the following available and complete the backup processes described before you proceed to upgrade the software:

- New software package.
- Current software image file (in case you need to reverse the upgrade).
- Backup of the configuration (the **configuration.xml** file).
- You will require the administrator user name and password for the configuration backup file if you ever need to use the backup. If you attempt to downgrade / restore the software and you cannot load an appropriate configuration file, you may be unable to log in to the device.
- If using Call Detail Records (CDRs), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When the device reboots as part of the upgrade, all existing CDRs will be deleted.
- Administrative access to all units to be upgraded.
- The model numbers and serial numbers of your devices in case you need to contact Cisco Technical Support.

CAUTION: Make sure that all the backup processes described in this section have been completed before you start the upgrade. Failure to do so could result in data loss.

CAUTION: If you are upgrading a cluster you must upgrade all blades in the cluster to the same software version.

Note: While you are upgrading a cluster, or restarting it for another reason, the master cannot report the cluster's full capacity until the slaves have also restarted. Any devices that poll the master for such information should check that the slaves are back up before assuming that the capacity has permanently been reduced, or that there is some other fault in the cluster.

Backing up your configuration

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
3. Go to **Configuration > Upgrade**.
4. In the **Back up and restore** section, click **Save backup file**.
5. Copy the resulting **configuration.xml** file to a secure location.

CAUTION: You must remember the administrator user name and password for the configuration backup file in case you ever need to use the backup.

Upgrade instructions

1. Unzip the image file locally.
2. In a web browser, navigate to the web interface of the device.
3. Sign in as an administrator.
   The username is *admin* and there is no password on a new unit.
4. Go to **Configuration > Upgrade**.
5. In the **Main software image** section, locate the **New image file** field. Browse to and select the unzipped new image file.
6. Click **Upload software image**.
   The web browser uploads the file to the device, which may take a few minutes.

   Note: Do not browse away from the **Upgrade** page, or refresh the page, during the upload process – this will cause the upload to fail.

   A pop-up window displays to show upload progress. When complete, close the message. The web browser refreshes automatically and displays the message *Main image upload completed*.
7. Click **Shut down TelePresence Server**. This option will now change to **Confirm TelePresence Server shutdown**. Click to confirm.
8. Click **Restart TelePresence Server and upgrade**.
   The unit will reboot and upgrade itself; this can take up to 25 minutes.

   Note: You may be logged out due to inactivity. If this happens, log in again, go to **Configuration > Shutdown** and click **Restart TelePresence Server and upgrade**.
9. Go to the **Status** page to verify that your device is using the new version.
10. If necessary, restore your configuration; refer to the online help for details.

Downgrade instructions

If you need to reverse your upgrade, you can re-install the former version of the software. The downgrade procedure is the same as the upgrade procedure except you will use the earlier software image.

CAUTION: Make sure that all relevant backup processes described in Prerequisites [p.27] have been completed before you start the downgrade. Failure to do so could result in data loss.

Downgrading from 3.1(1.95)

You need the correct target version of the software and the corresponding saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image.
2. Restart the hardware and check the status via the web interface.
   The status report indicates the software version.
3. Restore your configuration from the saved XML file; refer to the online help for details.

Upgrading the font (optional)

Note: These instructions apply only to TelePresence Server 7010 and MSE 8710 platforms. The Media 310/320 platforms always have the font pre-installed and there is no way to replace or remove it.

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

If the font is not present, and you want to use TrueType text rendering on your device instead of the default text rendering method, you must upload the font file. You can get this file, called **ts-font_3_0_2_48**, from the Software download page for 3.0(2.48).

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

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
   The username is *admin* and there is no password on a new unit.
3. Go to **Configuration > Upgrade**.
4. Under **Font upgrade** at **New font file** browse to locate the downloaded font file.
5. Select the font file.
6. Click **Upload font**.
   After a short while, the **Font file status** changes to *Present*.

Removing the font

1. If you want to revert to the default text rendering, click **Delete font**.
2. Confirm that you want to remove the font file.
   The **Font file status** changes to *Not present*.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the Search field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Getting help

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

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

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

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

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit http://www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document revision history

Date	Revision	Description
October 2013	10	3.1 Maintenance release
August 2013	07	3.1 Release