Cisco TelePresence Server Version 3.0(2.49)

Software Maintenance Release Notes

May 2014

Contents

Product documentation

The following documents provide guidance on installation, initial configuration, and operation of the product:

http://www.cisco.com/en/US/products/ps11339/tsd_products_support_series_home.html

New features in version 3.0(2.46)

Telepresence Interoperability Protocol version 8 (TIP v8)

Version 3.0(2.46) added support for TIP v8. This feature does not have any user interface controls or visibly apparent behavior changes.

The TelePresence Server will advertise TIP v8 and will act on received TIP v8 messages as appropriate. Enhancements to the negotiation of the content video channel using TIP v8 are not supported in version 3.0(2.46).

This feature is backwards-compatible with TIP versions 6 and 7.

New features in version 3.0(2.24)

The new features introduced in version 3.0 are only accessible when the TelePresence Server is remotely managed, for example by Cisco TelePresence Conductor (version XC2.0 or later). Remotely managed mode is implemented by the new 3.0 API.

- Remotely managed operation mode
- Advanced Remote Management API
- Dynamic optimization of resources SD licensing model
- FullHD content
- Chair and guests in conferences
- Automatic disconnection

Remotely managed operation mode

In this release the TelePresence Server can be configured to run in one of two modes. In locally managed mode all the current functionality and behavior of the TelePresence Server is retained including the current API. This is the default setting that takes effect on upgrade, so there is no loss of functionality when upgrading to version 3.0. But note that none of the new features listed here are available in locally managed mode.

This release introduces the ability to remotely manage the TelePresence Server, via the new remote management API. This API gives unprecedented control over configuration and resource usage on the TelePresence Server, enabling remote management systems to manage all aspects of day-to-day operation. For more details see the feature descriptions below.

In remotely managed mode responsibility for configuring and controlling the TelePresence Server is handed off to a remote management system such as the Cisco TelePresence Conductor (version XC2.0 or later). There must be a remote management system in place in order for the TelePresence Server to work in remotely managed mode because various features are no longer possible via the TelePresence Server's web interface. It is not possible to add conferences or call out to participants via the web interface when in remotely managed mode, since the remote management system controls those resources. Also note that OneTable mode is not supported in remotely managed mode.

In addition, in remotely managed mode the current API is no longer available. That means that any systems which use that API will no long be able to query and control the TelePresence Server, including the Cisco TelePresence Management Suite (TMS) and Cisco TelePresence T1 and T3 systems. TMS can continue to manage the TelePresence Server if it is configured to use the Cisco TelePresence Conductor (version XC2.0 or later). T1 and T3 systems can continue to join and take part in conferences, although some advanced call features are not available when the TelePresence Server is remotely managed. These include the ability to escalate a point-to-point call into a conference, to change the conference layout, to see participant lists and to remove people from the conference.

This new mode of operation is accessed and configured via the Web user interface **Configuration > Operation mode**. Note that **Operation mode** also gives the option to select *Locally managed* mode so the TelePresence Server can still be used in standalone mode.

CAUTION:

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

Advanced remote management API

The TelePresence Server supports a new remote management API which gives unprecedented control over calls and resource usage. This new API is only available when the TelePresence Server is in remotely managed mode and is used in place of the current API (see above). The new API features:

- Advanced URI configuration, enabling individual calls to be matched to specific sets of attributes

- Fine-grained configuration, so that options that previously had to be enabled or disabled for every participant within a conference or across a TelePresence Server can now be set on a per-participant basis
- Dynamic resource optimization, so that resource usage can be reported and managed in real-time across all calls on a TelePresence Server
- Access to new functionality, including chair and guest roles within conferences and automatic disconnection of participants (see below)

For full details of the 3.0 API please refer to Cisco TelePresence Server 3.0 API Reference Guide.

Dynamic optimization of resources

In previous releases the TelePresence Server had fixed port counts with set maximum resolutions. Any call connecting to the unit would use up a port, even if it was a lower resolution and required fewer resources. For instance, a 720p call requires half the resources of a 1080p call. But with a TelePresence Server in FullHD mode both a 720p call and a 1080p call would use the same number of resources when they connected, one FullHD port each.

In this release, when the TelePresence Server's operation mode is configured to be remotely managed via the new API, its resources can be optimized dynamically by a remote management system. This means that calls can connect and only use the resources they require, giving the most efficient use of blade resources across the different media types (i.e. audio, video, content) of different participants.

The screen licenses are apportioned into different fractions depending on the media type that participants are using. For example, a 1080p participant with 720p15 content and stereo audio would utilize 1 screen license. For other typical calls, refer to Table 1 below (note that the fractions of screen licenses listed here are the only ones available):

Table 1: Example calls and screen license costs

Main video	Audio	Content	Screen Licenses
480p30	Mono	In main video	¼
480p30	Stereo	720p5	⅓
720p30	Stereo	720p5	½
720p30	Stereo	720p30	1
1080p30	Stereo	720p15	1
720p60	Stereo	720p15	1
1080p30	Stereo	720p30	1 ½
1080p30	Stereo	1080p30	2
Dual-screen 1080p30	Stereo	720p30	2
Three-screen 1080p	Multichannel	720p30	3
Three-screen 1080p	Multichannel	1080p30	4
Four-screen 1080p	Stereo	1080p30	4

Note that one screen license enables one 1080p call with stereo audio and 720p15 content, the same as was enabled in FullHD mode in previous versions. One screen license also enables two 720p30 calls with stereo audio and 720p5 content, the same as was enabled in HD mode in previous versions. With no screen licenses a single 8710 or 7010 can accept 10 audio only calls, and can have up to twelve screen licenses applied. This means there is no loss of functionality compared to previous versions. The new flexible port licensing enables the same calls as were possible in previous versions, but the resources can now be optimized dynamically among them. Additionally the new flexible port licensing also offers lower resolution service levels, such as SD, which enables more calls per unit. These additional new service levels allow more control over capacity and can increase the number of calls. Note also that currently no two- or four-screen endpoints support multichannel audio.

The TelePresence Server can take any call at any supported resolution in to any conference (dependent upon the availability of screen license capacity and the number of calls supported by the TelePresence Server). If there is insufficient screen license capacity for a call then the call is rejected. Up to 12 screen licenses can be applied to a

TelePresence Server, applying any more than that does not enable any extra resources due to the limit on the available resource each TelePresence Server can allocate. To allow resources to be managed between conferences, the resources assigned to each call can be capped. If an endpoint with higher capabilities joins that conference, only the assigned resources are used.

The screen licenses on each blade in a cluster are summed, and that total is applied to the cluster overall. Therefore a four blade cluster can have up to 48 screen licenses applied to it, and can take up to 48 1080p calls with stereo audio and 720p15 content. Each blade can also take 10 audio-only calls each, so a four blade cluster can take up to 40 audio only calls in addition to the 48 1080p video calls. At lower resolutions more video calls are possible, up to the overall limit of 104 calls across a cluster including audio calls, the same as in previous versions. This is summarized in Table 2 below:

Table 2: Maximum numbers of calls on TelePresence Server clusters (12 screen licenses per blade)

Cluster size	SD	HD	FullHD
1 blade	48 SD calls, 10 audio-only calls	24 HD calls, 10 audio-only calls	12 FullHD calls, 10 audio-only calls
2 blades	96 SD calls, 8 audio-only calls	48 HD calls, 20 audio-only calls	24 FullHD calls, 20 audio-only calls
3 blades	104 SD calls	72 HD calls, 30 audio-only calls	36 FullHD calls, 30 audio-only calls
4 blades	104 SD calls	96 HD calls, 8 audio-only calls	48 FullHD calls, 40 audio-only calls

Note that each blade can also take an intermediate number of HD calls, and can have an intermediate number of screen licenses applied. In addition, a conference can comprise any combination of SD, HD and FullHD calls, as listed in Table 2, and will dynamically optimize its resources to give the maximum possible number of connections in each scenario.

When setting up conferences, calls are given a quantity of resources to use. That can be set conference-wide, or on a per-call basis, based on the URI which a call dials to connect. Once calls are connected, the resources assigned to them can be optimized dynamically, For example, if a call is configured as 1080p but only comes in at 720p the system can reclaim the surplus resources and allocate for another 720p call. This optimization is not automatic and must be implemented in a remote management system, such as the Cisco TelePresence Conductor, in order to happen.

Telepresence Interoperability Protocol (TIP) can only be negotiated when the participant is allocated sufficient resources. One-screen TIP participants require at least the following resources: two mono audio channels, 720p30 main video, and 720p5 content. Three-screen TIP participants require at least the following resources: four mono audio channels (multichannel), three channels of 720p30 main video, and 720p5 content.

SD licensing model

In previous releases the TelePresence Server could only operate in fixed port-count modes. Each call would take up an HD or FullHD port, even if it was a standard definition call. In this release, when the TelePresence Server is remotely managed and has its resources dynamically optimized, SD calls take up fewer resources than HD calls. This means that more SD calls are possible with the same number of resources. For an example of how many calls are possible, see Table 2 above. In addition, mixtures of standard definition calls and high definition calls can connect to the TelePresence Server, and each call will only use the minimum resources required.

FullHD content

The TelePresence Server now supports FullHD content resolutions, 1080p30 video. Any endpoint which negotiates that resolution will be able to send and receive content at that level, subject to sufficient resources being assigned to this conference and this call (see Dynamic Optimization of Resources above). Content resolutions of up to 1920x1200 at 27fps are supported. Note that at present FullHD content is not supported in calls using the TIP protocol, for example to TX endpoints. Calls using the TIP protocol support sending and receiving content at up to XGA at 30fps, provided sufficient resources are assigned to the call.

Chair and guests in conferences

Participants can be configured as chairs or guests when they connect to a conference. This can be based on the URI they dial if they are calling in, or set as a parameter for the participant when calling out. Participants can be set to wait for a chair to join, so that if only guest participants with this option are present in a conference then they remain in a lobby screen, and no participant can see or hear any other participant until a chair joins. Participants also can be set to disconnect on chair exit. If only guests remain in a conference with this option after all the chairs have left, then they are disconnected.

Automatic disconnection

Participants can be set to automatically disconnect, so that if only participants with this option are left in a conference, then all participants are disconnected. This can be useful for calls to recording devices or other calls that are only useful so long as the conference is ongoing. Recording devices could have this option set, while a normal participant would have it unset. Then once all the participants in the conference have disconnected these calls will automatically disconnect.

New features in earlier versions

This section corrects an omission from the Cisco TelePresence Server release notes that accompanied version 2.3 of the software.

Previous participant list improvements

In TelePresence Server 2.2 and earlier releases, endpoint entries on the conference's previous participant list behaved as follows:

- configured endpoints remained on the list indefinitely (only removed if the endpoint was deleted using the web interface)
- non-configured endpoints remained on the list for 30 seconds after disconnecting
- the list could not be cleared/reset by the user

In TelePresence Server 2.3 and later releases, endpoint entries on the conference's previous participant list behave as follows:

- all types of endpoints remain on the list indefinitely
- the TelePresence Server may remove entries to conserve memory (a maximum of 208 previous participants are stored globally)
- the user can clear this list manually by clicking **Clear previous participants record** on the conference's status page

Resolved issues

The following issues were found in previous releases and are resolved in version 3.0(2.49).

Resolved since version 3.0(2.48)

Identifier	Summary
CSCuo21468	**Symptom:** The following Cisco Telepresence products: Cisco TelePresence Server 8710, 7010 Cisco TelePresence Server on Multiparty Media 310, 320 Cisco TelePresence Server on Virtual Machine include a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration and running TelePresence server software 2.3(x), 3.0(x) or 3.1(x) **Workaround:** Not currently available. Customers that do not require of the new functionality present on TelePresence server software 2.3(x), 3.0(x) or 3.1(x) may evaluate the possibility to downgrade affected devices to TelePresence server release 2.2, which is not affected by this vulnerability. **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the

Identifier	Summary
	following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved since version 3.0(2.46)

Identifier	Summary
CSCuf74309	In the previous release, in rare circumstances, the TelePresence Server could experience an unexpected restart when receiving an invalid bitstream from a particular endpoint. This issue is now resolved.
CSCuf64987	In the previous release, the TelePresence Server could intermittently fail to decrypt video coming from EX90 or C20 endpoints after a hold and resume, resulting in a black pane in place of the endpoint's video. This issue is now resolved.

Resolved since version 3.0(2.24)

Identifier	Summary
CSCue28183	In the previous release, some encrypted calls from Cisco TelePresence System endpoints (CTS) were incorrectly considered to be unencrypted by the TelePresence Server. This issue is now resolved.
CSCue28277	In the previous release, a TelePresence Server could fail when using all its resources to host very small conferences. This issue is now resolved.
CSCud73153	In the previous release, a console user would be unable to configure a static IPv4 address if the first octet was one of 32, 64, 128, 160, 191, or 192. This issue is now resolved.
CSCud79712	In the previous release, calls between the TelePresence Server and CTS endpoints showed greater packet loss than they did with prior versions. This issue is now resolved.
CSCue30743	In the previous release, the TelePresence Server could make an unencrypted H.323 call from a conference that required encryption but would fail to properly disconnect the call as it should. This issue is now resolved.
CSCue28500	In the previous release, encrypted three-screen TIP calls may not have been decrypted by the TelePresence Server under certain circumstances. This issue is now resolved.
CSCud97523	In the previous release, the TelePresence Server would sometimes show corruption in a 30 fps XGA presentation stream from certain endpoints. This issue is now resolved.
CSCue30584	In previous releases, the resolution choice and ClearVision scaling behavior, for low resolution / low bandwidth endpoints, was less precise than expected. This issue is now resolved.
CSCud81537	In the previous release, presentation from the TelePresence Server to either the C20 or EX60 endpoint would fail if the call was interworked by VCS (in the call path TS←H.323→VCS←SIP→Endpoint). This issue is now resolved.
CSCue30619	In previous releases, when not using the conference name as the SIP display name, the TelePresence Server used its old product name in the From header. This issue is now resolved.
CSCud79767	In the previous release, content sharing between the TelePresence Server and CUCM-registered C-Series endpoints was sometimes delayed by up to 10 seconds after starting the content. This issue is now resolved.
CSCud59258	In previous releases, SIP fast update INFO messages did not contain the stream ID for the main video stream. This issue is now resolved.

Identifier	Summary
CSCud79709	In the previous release, the port usage information, for a remotely managed TelePresence Server blade, was incorrectly reported in the Supervisor UI. This issue is now resolved.
CSCud07193	In the previous release, a reInvite from a CTS endpoint to the TelePresence Server could cause a renegotiation that resulted in call failure. This issue is now resolved.
CSCud79720	In the previous release, a participant importance change could temporarily cause a drop in the frame rate of that participant's video. This issue is now resolved.
CSCud99783	In the previous release, the TelePresence Server would not disconnect the remaining guests if the API disconnected the last chair, despite that **`disconnectOnChairExit`** was enabled. This issue is now resolved.
CSCue30565	In the previous release, in rare circumstances and under high API load, the TelePresence Server could become unresponsive. This issue is now resolved.

Resolved since version 2.3(1.57)

Identifier	Summary
CSCuc33620	In previous releases audio from an endpoint could become corrupted when an endpoint changed from mono to stereo to mono again. This could occur when an endpoint started presenting and stopped again. This issue is now resolved.
CSCud10087	In previous releases sending DTMF tones from an EX90 endpoint could cause the TelePresence Server to fail to decode subsequent audio. This issue is now resolved.
CSCub02707	In previous releases, if the TelePresence Server received invalid video data the system could become unstable. This release introduces enhanced checks to discard invalid data.
CSCuc74067	In this release the call participant default call-out protocol has changed from H.323 to SIP.
CSCub84636	In rare circumstances, when putting a call on hold very quickly after resuming it, media in the call may fail. This issue is now resolved.
CSCud08937	In previous releases, Cisco TMS did not immediately detect that a TelePresence Server in locally managed mode is available after rebooting. This issue is now resolved when the TelePresence Server is not part of a cluster. If the TelePresence Server is part of a cluster and the Cisco TMS does not detect and show the correct port count when a cluster restarts (issue identifier CSCud53982), a workaround is to do a Force Refresh on TMS.
CSCud79745	In release 2.3, the TelePresence Server registered conference Numeric IDs to the gatekeeper or SIP registrar for conferences that were locked. This issue is now resolved.
CSCud78984	In rare circumstances, encrypted SIP calls from endpoints registered to Unified CM could fail to send or receive content or the call could fail after holding and resuming the call. This issue is now resolved.
CSCud79742	In release 2.3, the participant media summary in the CDR log would consider encrypted channels to be unencrypted under some circumstances. This issue is now resolved.

Open issues

The following issues apply to this version of the TelePresence Server software.

Identifier	Summary
CSCub48355	DTMF tone suppression is not supported in this version of TelePresence Server. If a participant in a conference sends DTMF tones then these will be heard by other participants in that conference.
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.

Limitations

Full-screen view of single-screen endpoints changed

CTS 3000 endpoints are now added to the list of endpoints that are preferred full-screen. If you have previously used CTS 3000 endpoints and not used T3 endpoints then you may need to change the **Full-screen view of single-screen endpoints** setting on the **Configuration > Default endpoint settings** page from the default **`Dynamic`** to the correct setting **`Allowed`**.

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 please refer to the VCS Administrator Guide.

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.

Security status reporting

Due to the way the security status is signaled, in some cases the call security status reported on a TIP-capable endpoint may differ from the security status reported in a TelePresence Server conference.

Recommended VCS version X7.2

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.

Fast updates in TS – Conductor – Cisco UCM deployment

Cisco TelePresence Conductor releases prior to XC2.0.2 do not correctly forward fast update requests from the TelePresence Server to endpoints registered to CUCM, resulting in lost or blocky video from those endpoints. This issue only affects deployments with TelePresence Server version 3.0(2.48) and Conductor versions prior to XC2.0.2 (Issue identifier CSCue89279).

To work around this limitation, either upgrade Conductor to XC2.0.2, or later, when you upgrade to TelePresence Server 3.0(2.48), or do not upgrade TelePresence Server to 3.0(2.48) until the Conductor is upgraded.

Content corruption from Cisco TelePresence TX Series endpoints

The content channel from a Cisco TelePresence TX Series endpoint running TX6.0 software can become corrupted if large areas of the source content change rapidly (Issue identifier CSCue93467).

Interoperability

Cisco endeavors to make the TelePresence Server interoperable with all relevant standards-based equipment. While it is not possible to test all scenarios, the testing that the data below is based on covers the 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 this 3.0 release. 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 (TS) last as a general convention. References to 'TS' means either TS behind Conductor or TS on its own.

Call path phrase	Explicit call path description
SIP	Endpoint ←- SIP → TS. A registrar is used but not shown here.
H.323	Endpoint ←- H.323 → TS. A gatekeeper is used but not shown here.
H.323 to SIP interworking	Endpoint ←- H.323 → VCS ←- SIP → TS.
SIP to H.323 interworking	Endpoint ←- SIP → VCS ←- H.323 → TS.
CUCM to VCS H.323 interworking	Endpoint ←- SIP → CUCM ←- SIP → VCS ←- H.323 → TS.
CUCM to VCS/Conductor SIP	Endpoint ←- SIP → CUCM ←- SIP → VCS/Conductor ←- SIP → TS.
TIP	Endpoint ←- SIP → CUCM ←- SIP → VCS/Conductor ←- SIP → TS 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'.

Endpoint	Software	Comments
Cisco TelePresence C Series Cisco TelePresence MX Series Cisco TelePresence SX 20	5.1.4	Tested H.323 and SIP interoperability. • When C20 or C40 endpoints connect to the TelePresence Server via a VCS which is interworking the calls from SIP to H.323, then sending content to these endpoints will fail. To work around this issue use either H.323 or SIP throughout the call to avoid interworking. (Issue identifier CSCud81537)
Cisco Unified IP Phone 9971	9.3.1	Tested CUCM to VCS/Conductor SIP interoperability. • Video optimization will not work in interworked calls. (Issue identifier CSCtx16122)

Endpoint	Software	Comments
Cisco TelePresence System (CTS) 1300-47 Cisco TelePresence System (CTS) TX1300 Cisco TelePresence System (CTS) 3000, 3200 Cisco TelePresence System (CTS) 500, 1100, 1000 Cisco TelePresence TX9000 Series	1.9.2	Tested TIP interoperability. • When on a secure call using TLS, using audio add-in from a CTS endpoint is not supported in this release, and will cause the call to fail. While in that state, placing the call on hold and then resuming it resolves this issue. Audio add-in is supported for non-secure calls. (Issue identifier CSCub87163) • 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. (Issue identifiers CSCuf07863 and CSCuf03190) 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. Tested CUCM to VCS H.323 interworking. • Cisco recommends that you do not interwork CTS calls. Under rare circumstances video issues may be encountered.
Cisco Unified Personal Communicator	8.6(3)	Tested CUCM to VCS/Conductor SIP interoperability and CUCM to VCS H.323 interworking. • CUPC calls will use low video resolutions. (Issue identifier CSCud81937)
Cisco Unified Video Advantage	2.2.2	Tested CUCM to VCS/Conductor SIP interoperability; no issues found.
Cisco TelePresence E20	4.1.1	Tested SIP, H.323, CUCM to VCS/Conductor SIP interoperability and CUCM to VCS H.323 interworking. • 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 TelePresence EX Series	5.1.2	Tested CUCM to VCS/Conductor SIP, CUCM to VCS H.323 interworking, SIP, and H.323 interoperability. • Under some circumstances there is an echo from the EX90 when sending it stereo audio when on speaker. To work around this, turn off the directional audio on the TelePresence Server or use a headset. (Issue identifier CSCud79705) • When EX60 endpoints connect to the TelePresence Server via a VCS which is interworking the calls from SIP to H.323, then sending content to that EX endpoint will fail. To work around this issue use either H.323 or SIP throughout the call to avoid interworking. (Issue identifier CSCud81537)
Jabber Video for iPad	9.1	Tested SIP and H.323 to SIP interworking. • Transition from video to content or content to video may lead to transient video issues. (Issue identifier: CSCud64312)
Jabber Video for Telepresence	4.5.7	Tested SIP and H.323 to SIP interworking. • In some cases increasing resources for a call will result in low frame rate from the endpoint. (Issue identifier CSCud79739)
Jabber for Windows	9.0.5	Tested CUCM to VCS H.323 interworking and CUCM to VCS/Conductor SIP interoperability. No issues found.

Endpoint	Software	Comments
Lifesize Room 200	4.7.21	Tested H.323 and SIP interoperability: • TLS encrypted SIP calls are not supported between this endpoint and the TelePresence Server. (Issue identifier CSCtx91859) • The endpoint does not support SIP content. • H.263 codec is not supported between this endpoint and the TelePresence Server, H.264 is enabled by default. • H.261 codec is not supported by the endpoint in SIP calls (not default codec); use H.264 codec (enabled by default). • SIP calls out from the TelePresence Server to a LifeSize endpoint may exhibit garbled audio, in both directions, if the calling parties use the G.722.1.C codec. This is unlikely to occur unless the call cannot fall back on another codec. Try using a different codec to work around this issue.
Lifesize Team MP	4.1.1	Tested H.323 interoperability. • SIP calls to the TelePresence Server from this endpoint are not supported.
Microsoft Lync 2010 through Cisco TelePresence Advanced Media Gateway	4.0.7	Tested SIP and H.323 interworking interoperability, no issues found.
Cisco TelePresence MXP Series	F9.1.2	Tested SIP and H.323 interoperability. • Automatic content handover does not work if MXP tries to present immediately after another endpoint sends content. (Issue identifier CSCud64503)
Polycom HDX4500 / HDX8000	3.0.5-22695	Tested H.323 and SIP interoperability. • HDX does not support redial missed/rejected calls due to an endpoint limitation.
Polycom OTX	3.0.5	Tested H.323 and CUCM to VCS/Conductor SIP interoperability: • OTX does not support redial missed/rejected calls due to an endpoint limitation. • Low bandwidth calls are not supported
Polycom VVX 1500	4.0.2.11307	Tested H.323 and SIP interoperability. • VVX does not support redial missed/rejected calls due to an endpoint limitation.
Radvision Scopia XT1000-series	02.05.0406	Tested H.323 and SIP interoperability: • XT1000-series will adversely alter aspect ratio of H.263+ video (not default codec). H.264 is used by default. • Dialing out to the endpoint from the TelePresence Server may result in content not working. Dialing in works around this issue. (Issue identifier CSCtz21165) • Making a 60fps call at less than 2 Mbps is not supported. As a work around, use a higher bandwidth or disable 60fps on the endpoint.
Sony G Series PCS-G50	2.72	Tested H.323 interoperability; no issues found.

Endpoint	Software	Comments
Cisco TelePresence T3 / T1	TC5.1.0 / TCU 4.2.0	Tested H.323 interoperability. • PIN entry and layout changing will not function as the T1 and T3 do not support DTMF/ FECC to the TelePresence Server. • Note that some T1 and T3 functionality is not supported when the TS operates in Remotely Managed mode. For further details, refer to: Remotely managed operation mode on page 2.

Infrastructure

Equipment	Software	Comments
Cisco TelePresence Content Server	S5.3	Tested H.323 and SIP interoperability; no issues found.
Cisco TelePresence Conductor	XC2.0	Found with TelePresence Server 3.0(2.46). Fast update requests may not be forwarded by Conductor to endpoints in Cisco UCM deployments with Conductor versions prior to XC2.0.2 (CSCue89279).

Gatekeepers

Equipment	Software	Comments
Cisco TelePresence Video Communication Server (VCS)	X7.2	Increasing resources for a call that leaves the TS as H.323 and is interworked by the VCS to SIP can cause the call to fail. (Issue identifier CSCud64471)
Tandberg Gatekeeper	N5.2	No issues found.

Cisco Unified Communications Manager

Equipment	Software	Comments
Cisco Unified Communications Manager	7.1.5.10000-12	The following features are not supported when interoperating with this version of CUCM: • Autodetection of CTS endpoints • Trunking to CUCM
Cisco Unified Communications Manager	8.5.1.10000-26	No issues found.
Cisco Unified Communications Manager	8.6.1.10000-43, 8.6.2.10000-30	Calls to CTS or TX endpoints running software version 1.8 or higher may fail due to defect CSCtr70893, particularly in encrypted calls. This is resolved in Cisco Unified Communications Manager software revision 8.6.2.21900-5.
Cisco Unified Communications Manager	8.6.2.21900-5	No issues found.
Cisco Unified Communications Manager	9.0.1.10000-37	No issues found.

Updating to version 3.0(2.49)

Software dependencies

In the case of the TelePresence Server blade(s), the Cisco TelePresence Supervisor MSE 8050 (Supervisor) blade must be running 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).
- Back up 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.

Backup configuration instructions

Using the web interface

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** area, click **Save backup file**.
5. Copy the resulting *configuration.xml* file to a secure location.

Using FTP

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Connect to the device using an FTP client.
3. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
4. Copy the *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

Using the web interface

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 the **Restart TelePresence Server and upgrade** button.

   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.

Using FTP

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Unzip the image file locally.
3. Connect to the TelePresence Server using an FTP client.
4. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
5. Upload the image file to the root.
6. Reboot the hardware after the upload.

   You can reboot via the upgrade page on the web interface.

   The unit upgrades itself when it restarts.
7. Log in to the web interface and go to the **Status** page to verify that your device is using the new version.
8. If necessary, restore your configuration; refer to the online help for details.

Note: You can monitor the upgrade progress via the serial port.

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 have been completed before you start the downgrade. Failure to do so could result in data loss.

Downgrade procedure

You need the correct version of the software and your 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.

Upgrade the font (optional)

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]**, from the software download page, i.e. http://www.cisco.com/cisco/software/type.html?mdfid=283645287&flowid=21873

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.

Using the web interface

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*.

Using FTP

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Connect to the device using an FTP client.
3. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
4. Upload **[ts-font]** to the device and rename it to **font**, because the device expects a file called **font**.

   For example, enter the command `put [ts-font] font` at the ftp prompt.

   After a short while, the **Font file status**, on the web interface's upgrade page, 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 the 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
May 2014	08	Maintenance release 3.0(2.49)
April 2013	07	Maintenance release 3.0(2.48)
March 2013	06	Maintenance release 3.0(2.46)
December 2012	05	First release for 3.0
December 2012	04	Release Candidate2
November 2012	03	Release Candidate
November 2012	02	EFT2 release
September 2012	01	EFT release