Cisco TelePresence Server 2.3(1.58)

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 2.3

- Increased HD capacity
- New resource allocation model
- Directional audio
- Optimized single screen layouts
- Conference PINs
- TCP Signaling with Encrypted Media
- Default certificate update
- Display icon when any participants are not encrypted
- API additions

Increased HD capacity

This release provides increased HD capacity of up to 24 x 720p30 screens of video plus content and introduces a new resource allocation model.

New resource allocation model

This release supports a new resource allocation model as follows:

- One TelePresence Server screen license enables 1 x 1080p30 screen plus content or 2 x 720p30 screens plus content
- Maximum TelePresence Server capacity is achieved with 12 screen licenses in all modes
- Full HD Mode with 12 licenses supports 12 x 1080p30 or 12 x 720p60 screens of video plus content at up to 720p15 for each screen.
- HD mode with 12 licenses supports 24 x 720p30 or 24 x w448p60 screens of video plus content at up to 720p5 for each screen.
- Each video port is allocated a corresponding content port regardless of whether content is used

Note: if you have 16 screen licences applied to your 8710 blade, then a warning will appear in the supervisor Port Licenses page, saying that more port licenses are allocated than are required. This warning can be ignored, and can be removed by reducing the number of allocated ports to 12.

The following tables detail how these ports are allocated for the different definition modes supported by the software.

Port allocations by hardware type in HD Mode—720p30 screens of video plus content at up to 720p5

Hardware arrangement	Video ports	Content ports	Audio-only ports
7010	24	24	10
8710	24	24	10
Cluster of 2 8710s	48	48	20
Cluster of 3 8710s	72	72	30
Cluster of 4 8710s	96	96	8

Port allocations by hardware type in Full HD Mode—1080p30 screens of video plus content at up to 720p15

Hardware arrangement	Video ports	Content ports	Audio-only ports
7010	12	12	10
8710	12	12	10
Cluster of 2 8710s	24	24	20
Cluster of 3 8710s	36	36	30
Cluster of 4 8710s	48	48	40

Directional audio

Previous releases supported Directional Audio between any CTS3000 systems within a conference. This release enhances this feature to also support single screen stereo endpoints and multi-screen systems with separate audio streams per screen.

This feature ensures that the audio appears to emit from wherever a participant is displayed on the screen(s).

On single screen stereo endpoints this will result in participants displayed on the left of the screen being heard from the left, those displayed in the middle being heard from the middle, and those displayed on the right being heard from the right.

On multi-screen systems, for example a 3-screen room, this will result in participants displayed on the left screen being heard from the left of the room, those displayed on the middle screen being heard from the middle of the room, and those displayed on the right screen being heard from the right of the room.

Directional audio is always enabled.

Optimized single screen layouts

This release supports new single screen layouts and a change in the default behavior. In version 2.2 you could change the layouts when 2 people were in a conference; this release (version 2.3) allows you to select a layout at any time, however, it will only take effect when 3 or more people are in a conference.

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

This default setting can be overridden by a participant changing the layout selection using Far End Camera Control. It can also be changed via DTMF keys 2 and 8.

This release also supports different layout options for multi-screen systems that can send DTMF or Far End Camera Control, such as the Cisco TelePresence TX9000. On such endpoints two layouts are available: Single and ActivePresence. You can use DTMF keys 2 and 8 to alternate between these two layouts—this allows you to show or hide the overlaid panes at the bottom of the screen.

The new layouts that can be sent to single screen endpoints are:

Single screen layout	Single-screen layout description
	Single: Endpoints will be shown in one full screen pane. The active pane is shown for multi-screen endpoints.

Single screen layout	Single-screen layout description
	ActivePresence: Endpoints will be shown in one full screen pane with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen. For multi-screen systems the active pane is shown in the main screen whilst the entire room is shown in the smaller panes.
	Prominent: Endpoints will be shown in one large pane with additional participants appearing in up to four equally sized panes at the bottom of the screen. For multi-screen systems the active pane is shown in the main screen whilst the entire room is shown in the smaller panes.
	Equal: Endpoints will be shown in a grid pattern of equally sized panes on the screen, up to 4x4. For multi-screen systems the entire room is shown as a multi-width pane.

Conference PINs

This release adds PIN control to conferences for incoming calls only. PINs can be configured via the web interface or the API. A maximum of 40 digits is supported. Setting a PIN when adding a new conference allows you to restrict access to that conference.

On entering the conference the participant will be presented with a PIN entry screen and an audio prompt. The PIN can then be entered via DTMF.

TCP Signaling with Encrypted Media

The TelePresence Server supports the use of encryption with SIP. When encryption is in use with SIP, the audio and video media are encrypted using Secure Real-time Transport Protocol (SRTP). When using SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDES).

In previous TelePresence Server releases, encryption was only ever used in conjunction with a secure transport for call control messages, such as the SDES key exchanges. Transport Layer Security (TLS) was used for that secure transport.

In certain network deployments using a secure transport may not be desired. To support such scenarios, this release adds a configuration option to support media encryption with any available transport mechanism for call control messages.

The recommended, and default behavior, will remain to use a secure transport. Extreme care should be taken before changing this configuration option as keys will be exchanged in clear text.

Default certificate update

In this release the TelePresence Server default certificate has changed. If any external devices were programmed to accept that certificate, such as T1 or T3 TCUs, these devices will need to be updated. See page 9 of the TCU Administrator Guide for details. Cisco strongly recommends that administrators do not use the default certificate as shipped, but instead supply their own certificate.

Display icon when any participants are not encrypted

In this release an icon is displayed to encrypted endpoints to indicate when an unencrypted call is in a conference. This is enabled by default.

API additions

This release includes API additions, such as:

- device.query
- device.network.query
- device.health.query
- device.restartlog.query
- device.restart

Many new parameters are also included for existing requests. For a full list of additions, please refer to the API Change Summary on page 5 of the Cisco TelePresence Server API 2.3 Product Programming Reference Guide.

Resolved issues

The following issues were found in previous releases of Cisco TelePresence Server and are resolved in version 2.3 (1.58).

Resolved since version 2.3(1.57)

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

Resolved since version 2.3(1.55)

Identifier	Summary

Identifier	Summary
CSCuc11343	In previous releases when performing a hold and resume of SRTP encrypted calls, occasionally the TelePresence Server would stop decoding incoming video from that endpoint, resulting in other endpoints in the conference seeing a black video pane from this participant. This issue is now resolved.

Resolved since version 2.2(1.54)

Identifier	Summary
CSCtx86237	In previous releases, under very rare circumstances, black panes could be shown in conferences when run on clustered TelePresence Servers. This issue is now resolved.
CSCtr91138	In previous releases, under very rare circumstances black panes or frozen video could be seen when lower resolutions (e.g. 720p30) were scaled up to full HD resolutions (e.g. 1080p30). This only occurred when the TelePresence Server was running in Full HD mode when a participant that was receiving Full HD video from the TelePresence Server was viewing a participant that was sending a lower resolution to the TelePresence Server full screen. This issue is now resolved.
CSCub32129	In some circumstances, the TelePresence Server stopped responding to HTTP(S) requests on both the web interface and API calls. This recent problem has been attributed to Firefox browser version 14.0.1 and is improved in this release (the first release code of Firefox 14; release date: 17th July 2012). This version of Firefox is still not recommended; Firefox 15 should be used instead (release date: 28th August 2012). See also the limitations section of these release notes.
CSCub02707	Under rare circumstances when receiving invalid video data the TelePresence Server could reboot unexpectedly. This is now resolved.
CSCub02752	In very rare circumstances, an unexpected reboot would not provide full debug information. This is now resolved.
CSCua55142	Some calls from a Polycom HDX system through a Cisco CTX would be disconnected. This issue is now resolved – these calls will connect even if TIP negotiation is abandoned or fails.
CSCub36506	Content video in SIP calls to some Polycom HDX endpoints would appear corrupted. This is now resolved.
CSCtz01891	In previous releases the TelePresence Server could continue to send SIP messages to old destinations and not use updated information within the SIP contact header. This issue is now resolved.
CSCtx68139	In previous releases RTCP Picture Loss Indication messages sent out by the TelePresence Server were dropped by the (Cisco) SBC with errors about "Badly formatted RTCP". This issue is now resolved.
CSCtz80493	Prior to this release, when some SIP endpoints went on hold it resulted in frozen video being displayed from that endpoint to other endpoints in the conference. This was dependent on the hold mechanism used by the endpoint. For example, the issue was seen with EX series, E20, Movi and MXP endpoints. This issue is now resolved.
CSCtz21092	In previous releases Static Locked Meetings did not Unlock when the last endpoint left the conference. This issue is now resolved.
CSCtw63907	In previous releases SIP failed to re-register to a second address when 2 addresses were returned by DNS SRV. This issue is now resolved.
CSCty06854	In previous releases the TelePresence Server did not open audio to a SIP endpoint via a combination of CUCM, CTX and SBCs such that AAC-LD was the only available audio codec and the 'user-agent' field was absent from the incoming SIP INVITE message. This issue is now resolved.

Identifier	Summary
CSCtr85049	In previous releases, a video port was used when using SIP to make audio-only calls to the TelePresence Server. This issue is now resolved.

Open issues

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

Identifier	Summary
CSCub84636	In rare circumstances, when putting a call on hold very quickly after resuming it, media in the call may fail. This will be addressed in a future release.
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.

Deprecated features

This section details features that are no longer supported in this release.

Experia support

Experia is a legacy Tandberg immersive system that was made 'end of life' in 2009. It has been superseded by the new Cisco Immersive TelePresence room systems. Experia endpoints will no longer be supported from this release.

Rooms support

Previous releases of the TelePresence Server had a room configuration option that allowed limited user customization and control via the web UI. This feature has been removed in this release.

Conference controller

Previous releases had the concept of a Conference Controller which could control and monitor a number of other TelePresence Servers. This feature has been removed in this release. Clustering of TelePresence Server blades is the supported method going forward.

Limitations

MTU setting

Setting an MTU value of less than 1000 is not recommended. This setting should be left at the default of 1400 unless there are specific reasons within the network for altering it.

Full-screen view of single-screen endpoints changed

CTS3000s are now added to the list of endpoints that are preferred full-screen. If you have previously used CTS3000s and not used T3 endpoints then you may need to change the setting 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 additionally 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 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

Currently slot 10 does not support clustering.

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 signalling is used throughout the call signalling path. This ensures that the call is fully secure.

Audio add-in on secure CTS calls

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.

Security status reporting

Due to the way the security status is signalled, 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.

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 2.3 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.

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 SIP	Endpoint ←- SIP → CUCM ←- SIP → VCS ←- SIP → TS.
TIP	Endpoint ←- SIP → CUCM ←- SIP → VCS ←- 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	5.1.0	Tested H.323 and SIP interoperability; no issues found.
Cisco Unified IP Phone 9971	9.2.4	Tested CUCM to VCS SIP interoperability; no issues found.
Cisco TelePresence System (CTS) 1300-47	1.9.1	Tested TIP interoperability; no issues found. Tested CUCM to VCS H.323 interworking. • Cisco recommends that you do not interwork CTS calls. Under rare circumstances video issues may be encountered.

Endpoint	Software	Comments
Cisco TelePresence System (CTS) 3000	1.9.1	Tested TIP interoperability; no issues found. 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 TelePresence System (CTS) 500	1.9.1	Tested TIP interoperability; no issues found. 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	8.5(3)	Tested CUCM to VCS SIP interoperability; no issues found.
Cisco Unified Video Advantage	2.2.2	Tested CUCM to VCS SIP interoperability; no issues found.
Cisco TelePresence E20	4.1.1	Tested SIP, H.323, CUCM to VCS SIP and CUCM to VCS H.323 interoperability. • 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 EX90	5.1.2	Tested CUCM to VCS SIP and CUCM to VCS H.323 interoperability; no issues found. • Echo from EX90 when sending it directional audio (only when on speaker). To workaround this, turn off the directional audio on the TelePresence Server or use a headset.
Jabber Video for Telepresence	4.4	Tested SIP and H.323 interworking interoperability; no issues found.
Jabber for Windows	9.3	Tested SIP and H.323 interworking interoperability; no issues found.

Endpoint	Software	Comments
Lifesize Room 200	4.7.18	Tested H.323 and SIP interoperability; known limitations: 1. TLS encrypted SIP calls are not supported between this endpoint and the TelePresence Server. (Issue identifier CSCtx91859) 2. The endpoint does not support SIP content. 3. G.722.1 audio is not supported between this endpoint and the TelePresence Server. 4. H.263 codec is not supported between this endpoint and the TelePresence Server, H.264 is enabled by default. 5. G.728 codec is not fully supported between this endpoint and the TelePresence Server, AAC-LC is enabled by default. 6. H.261 codec is not supported by the endpoint in SIP calls (not default codec), use H.264 codec (enabled by default). 7. Under rare conditions lip synchronization may be poor during IPv6 calls. 8. 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; no issues found. • SIP calls to the TelePresence Server from this endpoint are not supported.
Microsoft Lync 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. 1. FECC negotiation can take several seconds on SIP calls. 2. Automatic content handover does not work if MXP tries to present immediately after another endpoint sends content.
Polycom HDX8000	3.0.4	Tested H.323 and SIP interoperability. • H.263 codec is not supported between this endpoint and the TelePresence Server. H.264 is used by default.
Polycom VSX 7000e	9.0.6.2	Tested H.323 interoperability. • Making an interworked call can result in the endpoint restarting.
Polycom VVX 1500	4.0.2.11307	Tested H.323 and SIP interoperability; no issues found. • H.263 codec is not supported between this endpoint and the TelePresence Server. H.264 is used by default.
Radvision Scopia XT1000-series	02.05.0208	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.

Endpoint	Software	Comments
Sony G Series PCS-G50	2.72	Tested H.323 interoperability; no issues found. • Automatic content handover is not supported between this endpoint and the TelePresence Server.
Cisco TelePresence T1 and T3	TC5.1.0/TCU4.2.0	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.
Cisco TelePresence TX9000 Series	1.9.1	Tested TIP interoperability; no issues found. Tested CUCM to VCS H.323 interworking. • Cisco recommends that you do not interwork TX calls. Under rare circumstances video issues may be encountered

Infrastructure

Equipment	Software revision	Comments
Cisco TelePresence Content Server	S5.3	Tested H.323 and SIP interoperability; no issues found.

Gatekeepers

Equipment	Software revision	Comments
Cisco TelePresence Video Communication Server (VCS)	X7.1	No issues found.
Tandberg Gatekeeper	N5.2	No issues found.
Polycom PathNav	7.00.03	No issues found.
GNU Gatekeeper	3.0.2	No issues found.

Cisco Unified Communications Manager

Equipment	Software revision	Comments
Cisco Unified Communications Manager	7.1.5.10000-12	The following TelePresence Server 2.3 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.

Updating to version 2.3(1.58)

Note: You **must** back up your configuration **before** upgrading to 2.3(1.58).

You must also remember the administrator user name and password for the backup configuration. You will need these if you ever need to make use of this backup file.

If you are using Call Detail Records (CDR), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When you reboot the TelePresence Server, as part of the upgrade, you will delete all existing CDRs.

Prerequisites and software dependencies

- You need the software package (zipped image file) for this version.
- You should have the true type font file if you want to improve the text rendering. You can get this file, called **ts-font**, from the same place where you download your software, i.e. http://www.cisco.com/cisco/software/type.html?mdfid=283645287&flowid=21873
- You should also have any licenses and feature keys you need for the upgrade.
- Take a backup of your current configuration and software package, including logs and keys.
- Make sure you have administrative access to the Cisco TelePresence Server(s) and the Cisco TelePresence MSE 8050 Supervisor that manages their chassis.
- If you are upgrading a cluster of TelePresence Servers, you must have access to all of them and you must upgrade them all to the identical build.
- Keep a list of the model numbers and serial numbers of your devices in case you need to contact support.
- Arrange a downtime window and notify users of when the service will be unavailable. The approximate duration of an upgrade is 10 to 20 minutes.

Upgrade via the web interface

1. Unzip the image file locally.
2. Log in to your TelePresence Server's web interface with administrative credentials.
3. 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 TelePresence Server, which may take a few minutes.

   Note: Do not browse away from the **Upgrade** page, or refresh the page, during the upload process. The upload may fail if you do.

   The web browser refreshes automatically and displays the message *Main image upload completed*. Close the message.
7. Go to **Configuration > Shutdown**. 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. This button only appears in the **Upgrade** page during this process.

   The unit will reboot and upgrade itself which takes a few minutes.

   Note: You may be logged out due to inactivity. If this happens, log in again, go to **Configuration > Upgrade** and click **Restart TelePresence Server and upgrade**.

9. Go to the **Status** page to verify that your TelePresence Server is using the new version.
10. Restore your configuration if necessary; refer to the online help for details.

Upgrade via FTP

1. Unzip the image file locally.
2. Connect to the TelePresence Server via ftp.
   For example, enter **ftp *IP Address*** at the command prompt, or use an FTP client with a graphical user interface.
3. Supply the administrator username and password.
   Username is **admin** without a password (on a new unit).
4. Upload the image file.
   For example, enter **put *ImageFilename*** at the ftp prompt.
5. Reboot the hardware after the upload.
   You can reboot via the upgrade page on the web interface or use the power button on the hardware.
   The unit upgrades itself when it restarts.
6. Log in to the web interface and go to the **Status** page to verify that your TelePresence Server is using the new version.
7. Restore your configuration if necessary; refer to the online help for details.

Notes

- FTP is generally more reliable for upgrades than the web interface.
- 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.

You need the correct version of the software and your 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.

Upgrade the font

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

If the font is not present, and you want to use TrueType text rendering on your TelePresence Server instead of the default text rendering method, you must upload the font file.

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

Uploading via the web interface

1. Browse to the TelePresence Server and log in.
2. Click the button to locate and select **ts-font** (e.g. **Browse** or **Choose file**, depending on browser used).
3. Click **Upload font**.

   After a short while, the **Font file status** changes to *Present*.

Uploading via ftp

1. Open an ftp prompt in the local folder where you downloaded the file **ts-font**.
2. Open the TelePresence Server and log in.
3. Enter the command `put ts-font font` at the ftp prompt.

   This command copies and renames the file because the TelePresence Server expects a file called **font**.

   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*.

The identifiers listed in these release notes will take you directly to a description of each issue.

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 <product name>, 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.

Document revision history

Date	Revision	Description
May 2014	D14956.03	Cisco TelePresence Server 2.3 Second maintenance release (2.3(1.58))
December 2012	D14956.02	Maintenance release
December 2012	D14956.01	Release notes revised to include resolved issues CSCtx86237 and CSCtr91138
September 2012	D14956	These notes accompany the release of version 2.3 of the Cisco TelePresence Server software.