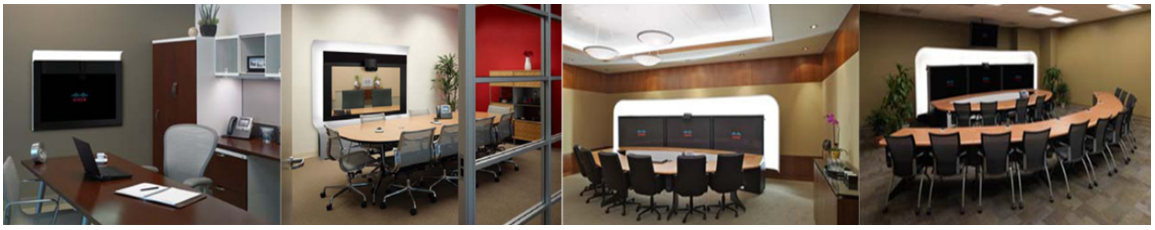

Release Notes for Cisco TelePresence System Software Release 1.8

Revised: December 4, 2012 OL-24611-01
CTS Release 1.8.5

Contents

These release notes describe new features and open and closed hardware and software caveats for the Cisco TelePresence System (CTS) software 1.8 releases, including the most current, CTS Release 1.8.5.

Note A copy of source code used in this product that is licensed under the General Public License Version 2.0 can be obtained by e-mailing a request to cts-gpl@cisco.com.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Important Notes

Observe the following important information for the Cisco TelePresence System:

Cisco Unified Call Manager 8.6.2 with CTS 1.8 720p Lite

When a CTS 1.8 endpoint that is configured to 720p Lite is registered to Cisco Unified CM 8.6.2, calls in secure mode sometimes drop. To work around this issue, either configure the CTS 1.8 720p Lite endpoint to non-secure mode or register the endpoint to Cisco Unified CM 8.6.1.

Adding or Removing a Presentation Codec

When you add or remove a CTS presentation codec in the system configuration, you must do so from the Cisco Unified CM Administration interface. After the configuration change is complete, click **Reset** to sync this configuration change with the CTS codec. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

ASR and GSR Support

Only Aggregation Service Router (ASR) 3.2 is supported with CTS Release 1.8.0. The Gigabit Switch Router (GSR) is not supported.

Audio Echo Cancellation (AEC) on the CTS 500-32 and CTS 500-37

The Enable Audio Echo Cancellation (AEC) checkbox in the Cisco Unified Communications Manager Administration is not available for CTS 500-32 and CTS 500-37 systems running Unified CM version 8.5 and higher. To enable or disable AEC on these systems, use the set audio aec disable and set audio aec enable command-line interface (CLI) commands, as shown in this example:

1. Enable or disable AEC:

```
admin:set audio aec disable

AEC support state changed to disabled
```

2. Restart calling services to have this take effect:

```
admin:utils service restart Calling_Services

Calling_Services   Restarting...done
admin:
```

3. Verify the configuration:

```
admin:show config all

Enable AEC              : Disabled
```

See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for more information.

Broadband Service Support

Customers can deploy Cisco TelePresence endpoints over Premium Broadband (Internet) such as business-class cable, FIOS, or E1 over the top. This gives customers flexibility to operate Cisco TelePresence across a variety of new connections.

All CTS endpoints and infrastructure must be upgraded to a minimum of Cisco TelePresence release 1.7 when broadband systems are deployed. Cisco TelePresence release 1.7 provides additional features to address the higher jitter and possible packet loss commonly found on broadband networks. Mixing CTS 1.7 systems with previous versions will disable the required CTS broadband network features, negatively affecting meeting quality, especially in multipoint meetings.

Calendaring on the Cisco TelePresence Touch 12

If the administrator leaves the roomName field blank in Cisco Unified Communications Manager Administration, the device calendaring features will not be managed by CTS-Manager. The Meetings button is not available on the touch device when the roomName field is blank.

Cisco TelePresence MIDlet File Naming Convention

When downloading MIDlet .jad and .jar files, use caution to avoid typos. Some files use a hyphen in the file string (“ **-** ”) and some use a period (“ **.** ”).

For example:

- TSPM-1.8.2-P1-1S.jar
- TSPM-1.8.2-P1-1S.jad

Note You must be running a minimum of Cisco Unified CM Release 7.0.2 to use MIDlets.

Cisco TelePresence T Series Endpoint Security

The Cisco TelePresence T Series endpoints do not register natively as secure endpoints; only non-secure mode is supported when talking to Unified CM.

Digital Media Player (DMP) Advisory

The DMP is always functional no matter the configuration on the Administration Web interface. The DMP Audio Administration configuration is set to indicate whether the audio will behave as a digital media player or as a PC; it does not turn the DMP capabilities on or off.

If the configuration is set to PC, the audio (whether coming from a DMP or a laptop) may be streamed to remote endpoints during a call. If the configuration is set to DMP, the audio (whether coming from a DMP or a laptop) may not be streamed to remote endpoints during a call.

The DMP button may not be visible after hours. See CSCtu19709.

Directory Settings in Unified CM

MIDlet does not support non UTF-8 characters so ensure that you use valid characters when updating the Directory feature in the Cisco Unified Communications Manager Administration interface.

End-of-Sale and End-of-Life Products

Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) for the following products

- Cisco announces the end-of-sale and end-of life dates for the Cisco TelePresence System 1000:

  http://www.cisco.com/en/US/prod/collateral/ps7060/ps8329/ps8331/ps7074/end_of_life_notice_c51-573606.html

- Cisco announces the end-of-sale and end-of life dates for the Cisco TelePresence System 3000 and Cisco TelePresence System 3200:

  http://www.cisco.com/en/US/prod/collateral/ps7060/ps8329/ps8331/ps7074/end_of_life_notice_c51-594068.html

Headset Support

Headsets are supported on the CTS 500 Series only.

Idle Display Field in Unified CM

Idle Display is a mandatory field in the Cisco Unified Communications Manager Administration interface. Specify any of the following options in the Idle Display field:

- Default Detailed

- Manual
- Directory
- Favorites
- Default Simple

Interoperability Updates

Security in a point-to-point call is supported between a CTS 1.8 endpoint and each of the following:

- Cisco TelePresence TC endpoint—Secure or non-secure, depending on the configuration of the Cisco TC endpoint.
- Cisco Unified IP Phones—Secure.
- Any of the Cisco interop endpoints listed in the matrix below—Non-secure.

For information on Cisco interop endpoints, see the Interoperability Between CTS Endpoints and Other Cisco Endpoints or Devices on Cisco.com.

Participant List Check Boxes

The check boxes next to active meeting participants on the Cisco TelePresence Touch 12 are view only; you cannot check or uncheck the entries.

Phone Screen Capture via Cisco Unified CM

Because the CTS codec is no longer the authentication server for the phone and cannot be used to obtain screenshots of the phone for diagnostics, you will need to create an End User profile to manage the phones and capture a screenshot. See the "Obtaining a Screenshot From the MIDlets Phone" section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Registering VLAN

If you want the CTS to autoconfigure itself with a VLAN without network interaction, set the Administrative VLAN in the Cisco TelePresence System Administration interface. To view or configure the administrative VLAN ID in the administration GUI, choose **Configuration > Network Settings**. See the Cisco TelePresence System Administration Guide for more information.

Resetting the CTS Factory Image

When you change the CTS model while performing configuration tasks in the administration interface (switching from a CTS 1000 to a CTS 1300-65, for instance), the CTS automatically reboots.

Resetting the Cisco Unified IP Phone 7975 Factory Image

Occasionally, an unexpected phone power cycle can occur during a CTS endpoint upgrade. During CTS endpoint upgrades, the CTS briefly powers off the phone then brings it back up when upgrade is complete. But if the phone power cycle is occurring at the same time, the phone's firmware image can be damaged and the phone will not power back on. This can also occur when upgrading the phone MIDlet.

To avoid this problem, schedule CTS endpoint or MIDlet upgrades when the phone is not in power cycle mode. If you encounter a phone that will not power back on after a CTS endpoint or MIDlet upgrade, perform a phone factory reset to restore the firmware image. For more information, see the Resetting the Cisco Unified IP Phone 7970 Series Factory Image section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

SCCP and SIP Phone Firmware Upgrades

For all SCCP and SIP firmware upgrades from firmware release versions earlier than 8.3(3) to version 8.5(3) or a later release, you must first upgrade your firmware to version 8.5(2). Once you have upgraded to version 8.5(2), you can upgrade your Cisco Unified IP Phone to version 8.5(3) or a later release.

See the Installation Notes section of the *Cisco Unified IP Phone Release Notes for Firmware Release 8.5(3) (SCCP and SIP)* for download instructions.

Setting the Device Type

By default the primary codec defaults to CTS 1000. To perform camera calibration on a CTS 3010/3020 if your system is not registered to the Unified CM, use the **set ctstype <3000 3010 ...)>** command. Whenever possible register your device to the Unified CM to configure the correct device type before calibrating the camera.

Single Microphone Mute

Single microphone mute is available with software upgrades beginning with Cisco Unified CM firmware release 8.0.3. This feature is configured using a disable/enable check box in the Cisco Unified CM Administration interface.

See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

SIP Max Incoming Message Size

You must set the SIP Max Incoming Message Size in Unified CM SIP to be greater than 5K. Otherwise it can cause issues with multiple hold/resume in interop calls with VCS and security. Cisco recommends setting it to 11000.

Updated Presentation Capability and Notification

If the remote endpoint does not support a 1024x768 presentation stream, the Not Sharing Presentation icon (a laptop with a slash through it) is displayed on the main screen along with the following message:

“Remote participant cannot receive presentation.”

While the CTS negotiates a lower frame rate, the following message appears:

“Please wait to receive video. Still sending video.”

Video resumes once the frame rate is negotiated. If the video takes longer to negotiate, the following message appears:

“Unable to receive video. Still sending video.”

Upgrading from a Cisco Unified IP Phone to a Cisco TelePresence Touch 12

For instructions on upgrading from a Cisco Unified IP Phone to a Cisco TelePresence Touch 12, see the “Upgrading From a Cisco Unified IP Phone to a Cisco TelePresence Touch 12” chapter of the *Cisco TelePresence Touch 12 User Guide.*

Upgrading from CTS Release 1.7 to CTS Release 1.8

Note If you are upgrading from any CTS release prior to 1.8.0 and using the Touch 12 device, refer to the “Understanding COP and Loads Files for the Cisco TelePresence System” chapter of the *Cisco TelePresence Touch 12 Installation Guide*.

When upgrading from any CTS 1.7 release to CTS Release 1.8.0, the system automatically upgrades slot 0 to CTS 1.8.0 if the existing CTS release in slot 0 is lower than CTS 1.8.0. Some systems upgrade more quickly than others:

- Cisco 3x00 Series, Cisco 1100, and Cisco 1300—Upgrade completes in approximately 1 minute and 30 seconds.
- Cisco 500-32 and Cisco 1300-47—Upgrade completes in approximately 4 minutes and 30 seconds.

Viewing Presentations on Laptops

The VGA cable interface requires a 60 hertz refresh rate, but some laptops receive 60hz but do not send 60hz. For best results when viewing presentation displays on your laptop, try the following:

- Perform an **Fn+F7** to disable the presentation first and then use **Fn+F7** to enable the presentation again (not necessary on Mac systems).
- Set the refresh rate in the monitor settings to something other than 60hz, then set it back to 60hz.
- Make sure that you have set your laptop resolution to 1024 x 768.

Web Access

To avoid having to start the Cisco TelePresence application manually after uploading the new image or restarting the CTS, make sure that web access has been enabled in the Cisco Unified Communications Manager Administration interface. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for more information.

Web Browser Support

Cisco administration interfaces are supported on Internet Explorer (IE) version 6 (recommended).

WebEx Presentation

If the Cisco TelePresence room already has a presentation cable plugged in once the Cisco WebEx client stops presenting, the display in the room switches to the Cisco WebEx welcome screen rather than to automatic presentation. Cisco TelePresence room presentation is automatically active only if the Cisco TelePresence room plugs in the presentation cable again after a remote participant has presented.

WebEx Presentations with Cisco TelePresence Touch 12

When a Cisco TelePresence room is in a Cisco WebEx meeting, once the Cisco WebEx client has stopped sharing a presentation, the Cisco TelePresence room must plug the presentation cable in or unplug it then plug it back in again for the Cisco TelePresence room to take over the presentation role.

What's New

The following sections contain new features in the Cisco TelePresence System 1.8 releases:

New Features in CTS Release 1.8.5

CTS software release 1.8.5 resolves system issues and enhances the user experience; there are no new features. See the "Caveats in CTS Release 1.8.5" section.

MIDlets Used With CTS Release 1.8.5

The following MIDlets can be used with CTS Release 1.8.5:

- TSPM-1.8.2-P1-1S.jar
- TSPM-1.8.2-P1-1S.jad

New Features in CTS Release 1.8.4

CTS software release 1.8.4 resolves system issues and enhances the user experience; there are no new features. See the "Caveats in CTS Release 1.8.4" section.

MIDlets Used With CTS Release 1.8.4

The following MIDlets can be used with CTS Release 1.8.4:

- TSPM-1.8.2-P1-1S.jar
- TSPM-1.8.2-P1-1S.jad

New Features in CTS Release 1.8.3

CTS software release 1.8.3 resolves system issues and enhances the user experience; there are no new features. See the "Caveats in CTS Release 1.8.3" section.

MIDlets Used With CTS Release 1.8.3

The following MIDlets can be used with CTS Release 1.8.3:

- TSPM-1.8.2-P1-1S.jar
- TSPM-1.8.2-P1-1S.jad

New Features in CTS Release 1.8.2

CTS software release 1.8.2 resolves system issues and enhances the user experience; there are no new features. See the "Caveats in CTS Release 1.8.2" section.

New Features in CTS Release 1.8.1

The following features are new in this release:

- VCS H.323 BFCP Support, page 9

Cisco TelePresence Multipoint Switch (CTMS) 1.8.1

CTMS Release 1.8.1 is available. See the Release Notes for the Cisco TelePresence Multipoint Switch, Release 1.8 on Cisco.com.

Codian MCU Support

CTS Release 1.8.1 supports the Cisco Multipoint Control Unit (MCU) 4500 Series. See the Cisco TelePresence MCU 4500 Series home page on Cisco.com.

VCS H.323 BFCP Support

CTS 1.8.1 supports enhancements to BFCP for point-to-point and multipoint Cisco TelePresence meeting presentations. See the following documentation on Cisco.com:

- Cisco TelePresence Release 1.8 Interoperability Deployment Guide
- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
- *Cisco Unified Communications Manager with Cisco VCS Cisco TelePresence Deployment Guide*

See also:

- Unified CM/Cisco VCS Security Support, page 13
- BFCP Backward Compatibility, page 16

New Features in CTS Release 1.8.0

The following features are new in this release:

- BFCP over UDP Collaboration Support, page 9
- Cisco TelePresence Call-In Number Feature, page 10
- Cisco TelePresence Touch 12, page 10
- Continuous Decode, page 11
- COP Files Download for Cisco TelePresence, page 12
- CTS-Manager, CTMS, and CTRS Release 1.8, page 12
- DHCP Option 60 Support, page 12
- Multiple Cisco WebEx Sites, page 13
- Security Enhancements, page 13
- Unified CM/Cisco VCS Security Support, page 13
- Watermark Removal, page 14

BFCP over UDP Collaboration Support

Binary Floor Control Protocol (BFCP) is used for controlling access to the media resources in a meeting. BFCP allows the CTS and the remote endpoint to view presentation and main display video simultaneously with improved presentation resolution for all third-party telepresence endpoints.

The CTS offers three media lines: one for audio, one for the main video, and the other for presentation or content using the session description protocol (SDP). Additionally, an application line is sent in the SDP for the BFCP control channel. The bandwidth of the presentation media line matches the capability of the CTS. For example, if the CTS is capable of 30 fps, the presentation media line bandwidth will be 4Mbps.

Note The CTS uses BFCP over user datagram protocol (UDP) in both secure and non-secure BFCP modes. BFCP is supported in CTS Release 1.8 and supports only Unified CM release 8.6.1.

To enable BFCP, the trunk from the Cisco Video Communication Server (VCS) to Unified CM must have a custom BFCP profile configured in the Cisco Unified Communications Manager Administration interface. This profile needs to be associated with every trunk and device that will use BFCP for presentation.

To configure BFCP for presentation, you must do the following:

1. Configure the Cisco VCS Zone for Unified CM.
2. Create a BFCP SIP profile in Unified CM and check the "Allow Presentation Sharing using BFCP" box.
3. Choose your new BFCP SIP Profile from the SIP Profile drop-down menu in the Protocol Specific Information field in Unified CM.
4. Restart all CTS endpoints.
5. Select the VCS trunk in Unified CM and set it to use BFCP.

See the following support documentation on Cisco.com:

- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
- *Cisco Unified Communications Manager with Cisco VCS Cisco TelePresence Deployment Guide*

See also:

- Unified CM/Cisco VCS Security Support, page 13
- BFCP Backward Compatibility, page 16

Cisco TelePresence Call-In Number Feature

The Cisco TelePresence Call-in Number feature enables a meeting organizer to allow users to join the meeting from Cisco TelePresence endpoints that are not scheduled in the meeting invitation. For more information, see the following documentation on Cisco.com:

- Release Notes for Cisco TelePresence Manager Release 1.8
- Release Notes for the Cisco TelePresence Multipoint Switch, Release 1.8
- Cisco TelePresence Call-in Number

Cisco TelePresence Touch 12

The Cisco TelePresence Touch 12 is a touch-panel LCD device that enables you to conduct telepresence meetings without the Cisco Unified IP phone. The Cisco TelePresence Touch 12 provides a consistent, natural interaction experience with all Cisco TelePresence models and acts as a foundation for meeting control that supports applications, services, and extensive collaboration possibilities.

The Cisco TelePresence Touch 12 requires CTS Release 1.8 or a later release and a minimum of Unified CM Release 8.5.1. Cisco TelePresence Touch 12 supports the following devices:

- CTS 3010
- CTS 3210
- CTS 1300 Series
- CTS 1100
- CTS 500 Series

For installation information and user support documentation, see the following documentation on Cisco.com:

- *Installing and Configuring the Cisco TelePresence Touch 12*
- *Cisco TelePresence Touch 12 User Guide*
- *Cisco TelePresence Touch 12 Meeting Quick Reference*

Note For instructions on upgrading from a Cisco Unified IP Phone to a Cisco TelePresence Touch 12, see the "Upgrading From a Cisco Unified IP Phone to a Cisco TelePresence Touch 12" chapter of the *Cisco TelePresence Touch 12 User Guide.*

See also:

- Enabling Directory Services For Systems That Are Running Unified CM 8.6.1
- Upgrading the CTS Software for Systems Running CTS Software Versions Prior to 1.7.4

Enabling Directory Services For Systems That Are Running Unified CM 8.6.1

To use the directory service for the Cisco TelePresence Touch 12, you must make the following changes in Cisco Unified Communications Manager (Unified CM):

1. Enable Cisco User Data Services on systems running Unified CM 8.6.1.
2. Configure the User Search Limit to 500.

Tip The Cisco TelePresence Touch 12 still functions if you do not enable User Data Services in Unified CM 8.6.1, but you cannot access the directory.

See the Configuring Cisco TelePresence Touch 12 Features in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for instructions.

Upgrading the CTS Software for Systems Running CTS Software Versions Prior to 1.7.4

See the following important software upgrade information in the Upgrading From a Cisco Unified IP Phone to a Cisco TelePresence Touch 12 document at the following URL:

http://www.cisco.com/en/US/docs/telepresence/peripherals/cisco_touch/installation/cisco_touch_installation_upgrade.html

Continuous Decode

The CTS codec is now able to decode most video resolutions on the main display and the presentation display. See Chapter 1, Interoperability in Cisco TelePresence Point-to-Point Calls in the *Cisco TelePresence Release 1.8 Interoperability Deployment Guide* at the following URL for a complete list of supported and tested send and receive resolutions:

http://www.cisco.com/en/US/docs/telepresence/interop/1_8/deployment/guide/Interop_Release1_8.html

COP Files Download for Cisco TelePresence

The Cisco Options Package (COP) file is a mechanism for installing files on a Unified CM in a secure manner. COP files are zipped .tar files that the Unified CM verifies, unzips, and untars so that the contents can be installed in the Unified CM from either a local or a remote source. Unified CM automatically extracts the codec and device files from the COP file and applies them to your Cisco TelePresence system.

Tip Systems that are running Cisco TelePresence System software release 1.7.4 or 1.7.5 can use a COP file to upgrade and install their software with limited feature support. Full feature support is available in CTS Release 1.8.0. CTS Release 1.7.4, 1.7.5, and 1.8 continue to support .sbn and jar/jad files.

Find the COP file in the "Download" section of the Cisco support site for your product, located at the following URL:

http://www.cisco.com/cisco/web/support/index.html

For more information about installing COP files in Unified CM, see the following documentation on Cisco.com:

- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
- Understanding COP Files for the Cisco TelePresence System

CTS-Manager, CTMS, and CTRS Release 1.8

Release 1.8 introduces new features such as the following:

- CTMS running on the Cisco UCS C210 M2 using VMware
- CTS-Manager clustering
- Interoperability with MXE 5600 and Content Sharing
- Multiple CTMS devices can be deployed in a Cisco TelePresence topology
- Record meetings with multiple video and audio streams
- TelePresence Server Scheduling: Now supported for scheduling multipoint meetings
- User delegation to allow other users to manage meetings

For more new feature information, see the following documentation on Cisco.com:

- Release Notes for Cisco TelePresence Manager Release 1.8
- Release Notes for the Cisco TelePresence Multipoint Switch, Release 1.8
- Release notes for Cisco TelePresence Recording Server, Release 1.8

DHCP Option 60 Support

DHCP vendor class identifier option 60 identifies and associates a DHCP client with a particular vendor. Administrators can provision their systems with DHCP option 60 when providing converged services in their network environment. DHCP option 60 is enabled on a customer's DHCP server by the customer's administrator.

Multiple Cisco WebEx Sites

To allow more Cisco WebEx users to access meetings remotely, you can configure up to five Cisco WebEx servers with your CTS-Manager account. The meeting organizer can register the CTS-Manager with any one of the five configured Cisco WebEx servers.

See the Cisco TelePresence System Manager home page for support documentation.

Security Enhancements

CTS Release 1.8 introduces the following security enhancements:

- Diffie-Hellman, page 13
- Secure Icon Behavior, page 13
- Session Parameters, page 13

Diffie-Hellman

To provide an additional level of security, Datagram Transport Layer Security (DTLS) clients will offer RSA as well as the Diffie-Hellman (D-H) key exchange mechanism. If the remote endpoint supports D-H, then the handshake is performed using D-H. The DTLS handshake with endpoints running releases prior to CTS Release 1.7.4 and 1.8 perform the handshake using RSA. This modification enables two CTS 1.7.4 or CTS 1.8 endpoints communicating with Unified CM releases prior to 8.5 to perform the DTLS handshake using D-H. The CTS uses the signaling path to exchange the fingerprints of the certificate used in the DTLS handshake. The certificate received in the DTLS handshake will be validated using the fingerprints.

Secure Icon Behavior

In certain calls involving a conference bridge, Unified CM downgrades a call status to non-secure. This could happen when a non-secure endpoint joins a conference, which has been secure. Unified CM sends SIP updates to the CTS indicating that the call is non-secure. CTS shows the secure or non-secure icon (closed or open padlock image) if the media is set up to use either of the following:

- SDP keys due to DTLS failure
- DTLS keys have been exchanged using fingerprint

Note The SIP updates are be ignored if the call is using DTLS keys but the DTLS handshake is setup without fingerprints.

Session Parameters

Secure Real-time Transport Protocol (SRTP) security defines a set of "session" parameters, which optionally can be used to override SRTP session defaults for the SRTP and Real-Time Transport Control Protocol (SRTCP) streams. These parameters configure an Real-time Transport Protocol (RTP) session for SRTP services. The session parameter provides information required to establish the SRTP cryptographic context for the session. The CTS negotiates the SRTP session parameter and honors the negotiated parameters.

Unified CM/Cisco VCS Security Support

CTS Release 1.8 introduces support for secure calls with the Cisco TelePresence EX and Cisco TelePresence C Series endpoints through Unified CM/Cisco VCS deployment.

The network is set up as follows: CTS > Unified CM > Cisco VCS > Cisco TC

To configure security, the following conditions must be met:

- You must be running the following software:
  - Unified CM 8.6 or a later release.
  - CTS endpoints—CTS Release 1.8 or a later release.
  - Cisco TC endpoints—Cisco TC5 or a later release.
- Both the CTS and TC endpoints must be running in secure mode and be securely connected to their respective call managers.
- The Cisco VCS and Unified CM must be connected through a secure trunk.
- You must choose **vcs-interop** in the Normalization Script window while configuring the trunk profile in Unified CM.

See the following support documentation on Cisco.com:

- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
- *Cisco Unified Communications Manager with Cisco VCS Cisco TelePresence Deployment Guide*

Watermark Removal

Broadcast customers who want to remove the Cisco logo from their video presentations when it interferes with on-screen elements can do so in the Unified CM Administration interface by downloading a broadcast license. Contact your account representative to obtain the license.

For more information, see the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Cisco TelePresence Software Compatibility Matrix

For complete Cisco TelePresence software compatibility information, see the software support matrix on the Cisco TelePresence Administration Software page at the following URL:

http://www.cisco.com/en/US/products/ps8332/products_device_support_tables_list.html

Supported Camera Firmware

Table 1shows the supported firmware for the Release 1.8 software.

Table 1 Minimum Required Camera Firmware by Product

Cisco TelePresence System	Minimum Required Camera Firmware
Cisco TelePresence System 500-32	1187
Cisco TelePresence System 500-37	479
Cisco TelePresence System 1000 Cisco TelePresence System 1300-65 Cisco TelePresence System 3000 Cisco TelePresence System 3010 Cisco TelePresence System 3200 Cisco TelePresence System 3210	462

Table 1 Minimum Required Camera Firmware by Product

Cisco TelePresence System	Minimum Required Camera Firmware
Cisco TelePresence System 1300-47	1006
Cisco TelePresence System TX9000 Cisco TelePresence System TX9200	1394

Caveats in the CTS 1.8 Releases

This section contains the following caveat information:

Cisco TelePresence System Expected Behavior, Known Issues, and Workarounds

The following is expected behavior or known issues in the CTS Release 1.8 releases:

Addressing with CTS Deployments

Deploying CTS endpoints in a network with both 10.x.x.x addresses and 192.168.x.x addresses may result in routing errors.

CTS endpoints reside on two networks simultaneously; an “external” network by which it communicates with other CTS endpoints and the internet, and an “internal” network by which it communicates with internal devices such as cameras, UI devices, etc. When a CTS endpoint comes up, it tries to pick an internal network address that does not conflict with the external network's address space. By default, it uses several RFC 1918 Class C subnets (192.168.xx) to address internal devices. In the event that the External network is based out of a network with the 192.168 prefix, a RFC 1918 Class A subnet (10.0.xx) is used to address the internal devices. When a CTS endpoint sends a packet, it chooses the most specific route in its routing table. Thus, if there exist two devices with the same IP address, where one is on the internal network while the other is on the external network, all packets emanating from the CTS will be sent to the internal network rather than the external network.

In this case, when the CTS on the right tries to send a packet to the CTS on the left, it will instead be routed (internally, by the CTS) to the Peripheral that is directly attached.

BFCP Backward Compatibility

BFCP is not supported in CTS software releases prior to CTS Release 1.8. BFCP is enabled by default on all CTS endpoints beginning with CTS Release 1.8. Endpoints using CTS software prior to CTS Release 1.8 must either disable BFCP on all new SIP profiles in the Unified CM Administration interface or upgrade all CTS endpoints to CTS Release 1.8.

Black Bar During Presentation

Some telepresence systems do not accept presentations at the recommended 1024x576 resolution. Occasionally a black bar is displayed during a presentation.

Cisco TelePresence EX Series “Best Effort” Audio-Addin Support

Non secure audio-addin calls are dropped from the Cisco TelePresence EX Series automatically when Encryption is set to On in the Cisco TelePresence EX Series administration. Go to **Configuration > Conference > Default Call > Encryption** and select “Best Effort” from the drop-down menu then click **Save** to allow audio-addin calls to continue. Secure call settings are still supported on the CTS endpoint but you must configure the Cisco TelePresence EX Series for Best Effort if your conference will include audio-addin calls, which are non secure by default.

Cisco TelePresence Touch 12 Troubleshooting

Sometimes the Incoming Call window overlaps the incoming call override button during troubleshooting or the Incoming Call window does not automatically disappear. This is a cosmetic issue. Tap the available Answer, Ignore, or iDivert buttons or simply allow the call to ring until it ends automatically. Configure iDivert in the Cisco Unified Communications Manager Administration.

Command-line Interface (CLI) Restrictions

Avoid using the following commands to collect call status logs while in an active call:

- **file tail**
- **ipsla**
- **tcpdump**

Using these commands during an active CTS call can cause high CPU usage and may bring calls down.

Cisco Unified IP Phone 7985

Cisco announces the end-of-sale and end-of life dates for the Cisco Unified IP Phone 7985G.

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/end_of_life_notice_c51-586306.html

There are known interoperability issues between the Cisco Unified IP Phone 7985 and the CTS 1300 Series; audio addin can cause the CTS main display to freeze.

Detect and Disconnect Audio Addin Calls

Occasionally an audio addin call remains listed on the meeting participant Conference List even though the call has dropped. Due to the call preservation feature, the CTS waits for the Unified CM to send a BYE message before dropping an audio addin call. The CTS can enact several mechanisms to detect when the audio addin has dropped, including dropping the call when the phone has been rebooted.

The CTS cannot support two audio addin calls at the same time.

Directory Entries for Cisco TelePresence Touch 12

When Directory entries are added or updated in the Cisco Unified Communications Manager Administration interface, an erroneous LASTNAME entry is listed on the Cisco TelePresence Touch 12. This is a cosmetic issue that does not affect functionality; there is no last name entry requirement in the administration interface for directory listings.

Document Camera Swap

Make sure that you reset your CTS any time that you swap document cameras that are running different firmware versions. See CSCtt93919.

Double-talk on the Cisco TelePresence System

During double-talk (when both sides are talking simultaneously), two things happen:

1. The audio from the remote side is slightly lowered before it is played out of the speaker.
2. Echo cancellation removes some of the sound from the talkers.

Endpoints That Cannot Share or Receive Presentations

Some telepresence endpoints do not support the ability to share or receive presentations. If you encounter an endpoint that does not support presentations, the CTS displays the following notification on the main screen:

“Remote participant cannot receive presentation”

Limited Bandwidth Mode: 360p

You may see the “Limited Bandwidth Mode: 360p” option in the Unified CM administration Quality (per Display) field. This choice will be available in a future release and is not available in CTS Release 1.8.

MXP Support on the Cisco TelePresence System

Observe the following notes about the Cisco TelePresence System MXP Series:

- The CTS sends 360p, receives 360p, and there is no presentation support.
- The CTS sends 360p, receives CIF, and bidirectional presentation is supported.
- The Cisco TelePresence System MXP 1000 SCCP does not support presentation.

Participant List Behavior in Large Meetings

A cosmetic issue occurs when there are more than five participants in the participant roster list on the Cisco Unified IP phone. Sometimes there are blank entries in the list as the user scrolls up and down to see the entire list. Feature functionality is not affected.

PiP Control

Some systems may show the Presentation-in-Picture (PiP) controls briefly while sharing presentations. Ordinarily PiP is not available during presentations. This is a cosmetic issue that occurs when the system tries to negotiate an unsupported DVI screen resolution.

Recording with Cisco TelePresence Touch 12

Sometimes the Cisco TelePresence Touch 12 active meeting screen flashes momentarily when the recording window is opened in preparation for recording the meeting. This is a cosmetic issue that corrects itself in a few seconds and does not affect functionality.

SDP and SRTP with CTS Release 1.7.4 and CTS Release 1.8.0

Customers who are deploying their B2B infrastructure with secure trunks to ASR/SBC secured by using TLS/Encryption, may experience call drops unless specific scripts are installed and configured on the ASR/SBC devices. Once the scripts and configuration are in place, certain SDP attributes are manipulated to enable SBC to unblock the SIP messages to and from Unified CM.

The following is an overview of the configuration steps:

1. Upload attached srtp.lua script to your ASR1k.
2. Define two SDP editors, for example to_rtp_avp and to_rtp_savp.
3. Configure a script set, as shown in the following example:

```
script-set 2 lua
    script srtp
      filename bootflash:srtp.lua
      load-order 100
      type full
    complete
   active-script-set 2
```

4. Use the SDP editor on both the inbound and outbound adjacencies:
   - Ask SBC to modify the SDP calling to_rtp_avp before-receive
   - And calling to_rtp_savp after-send

```
editor-type editor
    editor-list before-receive
     editor 1 to_rtp_avp
    editor-list after-send
     editor 1 to_rtp_savp
```

5. Create three editor headers:
   a. tp-to-x-supported
   b. tp-to-supported
   c. tp-add-x-srtp-fb

The first two are used in the inbound side, which will detect if any X-cisco-srtp-fallback tag gets into the supported header and then adds an srtp-fb header that includes the X-cisco-srtp-fallback tag (if present). The third one changes the internal srtp-fb header to the supported header prior to sending on the wire. The following is an example configuration:

```
adjacency sip peer2
    header-editor inbound tp-to-supported
    editor-list before-receive
     editor 1 to_rtp_avp
     editor 2 tp-to-x-supported

 adjacency sip peer1
    header-editor outbound tp-add-x-srtp-fb
```

See the following documents for support:

- Cisco ASR 1000 Series Aggregation Services Routers home page
- Business-to-Business Telepresence Configuration Profile Example

Sharing Presentations from the Cisco E20 IP Video Phone

The Cisco E20 IP Video Phone does not support BFCP for 1024x768 presentation and therefore the CTS cannot send presentations to the Cisco E20 (CSCtu75116).

CTS Release 1.8 Caveat Quick Reference

Table 2 summarizes caveats found in all CTS Release 1.8 releases. Use the CDETS number in this table to navigate to detailed descriptions.

Table 2 Caveats Quick Reference

CDETS Number	Software Release 1.8.5 Found in Release	Corrected in Release
CSCtx69209	1.8.4	1.9.0
CSCud33562	1.8.4	1.8.5
CDETS Number	**Software Release 1.8.4 Found in Release**	**Corrected in Release**
CSCtz40953	1.9.0	1.8.3
CSCtz38382	1.8.1	1.8.3
CSCub36142	1.9.0	1.8.3
CSCub48754	1.8.1	1.8.3
CDETS Number	**Software Release 1.8.3 Found in Release**	**Corrected in Release**
CSCtw50421	1.9.0	1.8.3
CSCtz97783	1.8.1	1.8.3
CDETS Number	**Software Release 1.8.2 Found in Release**	**Corrected in Release**
Resolved Caveats in CTS Release 1.8.2	1.8.2	—
CDETS Number	**Software Release 1.8.1 Found in Release**	**Corrected in Release**
CSCtx55737	1.8.1	—
CSCtx38646	1.8.1	—
CSCtx62312	1.8.1	—
CSCtx41146	1.8.1	—
CSCtw50738	1.8.1	—
CSCtx38628	1.8.1	—
CSCtx17774	1.8.1	—
CSCtu75116	1.8.0	—

Table 2 Caveats Quick Reference (continued)

CSCtx19741	1.8.1	—
CSCtu82870	1.8.1	1.8.1
CSCtu07566	1.7.4	1.8.1
CSCtu24513	1.7.2.1	1.8.1
CSCtv17399	1.7.5, 1.7.6	1.8.1
CSCtz21799	1.8.1	1.8.2
	Software Release	
	1.8.0	
CDETS Number	**Found in Release**	**Corrected in Release**
CSCty56195	1.7.6	—
CSCtw93670	1.8.0	—
CSCtw45493	1.8.0	—
CSCtr92400	1.8.0	—
CSCtq70191	1.7.4	—
CSCtt09629	1.8.0	—
CSCtt22889	1.8.0	—
CSCts33202	1.8.0	—
CSCto71973	1.7.4	—
CSCtq44109	1.8.0	—
CSCtq44157	1.8.0	—
CSCtu24860	1.8.0	—
CSCts29266	1.8.0	—
CSCtn40939	1.7.4	—
CSCtn50573	1.7.4	—
CSCtu25166	1.8.0	—
CSCtr15284	1.7.4	—
CSCts19075	1.8.0	—
CSCts27500	1.8.0	—
CSCts43318	1.8.0	—
CSCts47288	1.8.0	—
CSCts68292	1.7.5	—
CSCts80076	1.8.0	—
CSCts96560	1.8.0	—
CSCtt15735	1.8.0	—
CSCtt19841	1.8.0	—
CSCtt35671	1.8.0	—

Table 2 Caveats Quick Reference (continued)

CSCtt36038	1.8.0	—
CSCtu00932	1.8.0	—
CSCtu07566	1.7.4	—
CSCtu08086	1.8.0	—
CSCtu10328	1.8.0	—
CSCtu10835	1.8.0	—
CSCtu19709	1.8.0	—
CSCto89367	1.7.4	—
CSCts06855	1.8.0	—
CSCts64918	1.8.0	—
CSCtu19775	1.8.0	—
CSCts68355	1.7.4	—
CSCtu28325	1.8.0	—
CSCtn24147	1.7.2	—
CSCtr49077	1.7.4	—
CSCtu04961	1.8.0	—
CSCts56824	1.8.0	—
CSCtu07975	1.8.0	—
CSCtu07956	1.8.0	—
CSCtt94368	1.8.0	—
CSCtu07821	1.8.0	—
CSCtt93919	1.8.0	—
CSCtr72983	1.8.0	—
CSCts09587	1.8.0	—
CSCts09587	1.8.0	—
CSCtu00932	1.8.0	—
CSCtt19925	1.8.0	—
CSCtu19529	1.8.0	—
CSCts10775	1.8.0	—
CSCtw47775	1.8.0	—

Caveats in the Cisco TelePresence System

See the following sections for information about unexpected behavior found on the Cisco TelePresence System in the CTS Release 1.8 releases that use the CTS with the Cisco Unified IP Phone and MIDlets:

- Caveats in CTS Release 1.8.5, page 23
- Caveats in CTS Release 1.8.4, page 23
- Caveats in CTS Release 1.8.3, page 25

Caveats in CTS Release 1.8.5

Unresolved Caveats in CTS Release 1.8.5

CSCtx69209

Symptom The document camera power button on the Touch 12 device does not work after a CTS power cycle (turn off, then turn on).

Conditions After turning a CTS system off, then turning it back on, the Touch 12's document camera power button does not work.

Workaround Use VZ-C12[3] or VZ-9plus[3] document cameras, or upgrade to CTS software release 1.9.x.

Resolved Caveats in CTS Release 1.8.5

CSCud33562

Symptom Document camera image does not display on local projector screen.

Conditions This error occured after upgrading to CTS software release 1.8.4. When the document camera is in use, only the remote endpoint can see the document camera image, not the local endpoint.

Workaround There is no workaround.

Caveats in CTS Release 1.8.4

Resolved Caveats in CTS Release 1.8.4

CSCtz40953

A remote code execution vulnerability in the implementation of the Cisco Discovery Protocol (CDP) component could allow an unauthenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerability is due to a failure to properly handle malformed CDP packets. An attacker

could exploit this vulnerability by passing malformed CDP packets to an affected device. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code with elevated privileges.

Because CDP works at the data link layer (Layer 2), an attacker must have a way to submit an Ethernet frame directly to an affected device. This action may be possible in situations where the affected system is part of a bridged network or connected to a non partitioned device, such as a network hub.

This issue was disclosed in the following Cisco Security Advisories:

Cisco TelePresence Multipoint Switch

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctms

Cisco TelePresence Recording Server

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctrs

Cisco TelePresence Manager

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctsman

Cisco TelePresence Immersive Endpoint System

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-cts

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 8.3/7.5:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:U/RC:C

CVE ID CVE-2012-2486 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/en/US/products/products_security_vulnerability_policy.html

CSCtz38382

A remote command injection vulnerability exists in one of the Cisco TelePresence APIs that are hosted on the immersive endpoint devices. This issue, if exploited, could allow an unauthenticated attacker in an adjacent context to execute arbitrary commands on the underlying operating system with elevated privileges.

An attacker must have the ability to submit a malformed request to TCP port 61460 from a physical or logical Layer 3 adjacent context. A three-way handshake is required to exploit this vulnerability.

This issue was disclosed in the following Cisco Security Advisory:

Cisco TelePresence Immersive Endpoint Devices

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-cts

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 8.3/7.9:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C

CVE ID CVE-2012-3074 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/en/US/products/products_security_vulnerability_policy.html

CSCub36142

When a Cisco TelePresence System 3000 Series system that is registered to Cisco Unified Communications Manager (Unified CM) is sending video using a document camera, some EX series systems that are registered with a Video Communication Server (VCS) receive scrambled video.

CSCub48754

During either a point-to-point or multipoint meeting, when you conference in another Cisco TelePresence endpoint as an audio-only endpoint, you experience poor audio quality.

Caveats in CTS Release 1.8.3

- Resolved Caveats in CTS Release 1.8.3, page 25

Resolved Caveats in CTS Release 1.8.3

CSCtw50421

On rare occasions, in a point-to-point call between two CTS 3x00s, only the center screen displays video.

CSCtz97783

Inaccurate display error in the CTS web interface when the display goes from off state to standby state.

Caveats in CTS Release 1.8.2

- Resolved Caveats in CTS Release 1.8.2, page 25

Resolved Caveats in CTS Release 1.8.2

CSCtz21799

Symptom Cisco TelePresence systems display the time in UTC format instead of in local time.

Conditions This condition has been seen on the CTS 500-32 or CTS 1300-47 platforms.

Workaround There is no workaround.

CSCtz14870

Symptom Display firmware not being upgraded.

Conditions On systems with Sampo F13 65” diplays running display firmware version 31.46, the firmware is not upgraded to verion 31.47 when CTS Release 1.8.2 is installed.

Note To determine if a Sampo F13 65” display is installed on a CTS endpoint, log into the CTS Administration software, and from the Device Information page, click System Information Details button. A Sampo F13 display will show “SMP” as the first three characters in the Display_Serial field, and will show “CTS-DISP-65-GEN4” in the Display_Model field.

Workaround There is no workaround.

Caveats in CTS Release 1.8.1

Unresolved Caveats in CTS Release 1.8.1

CSCtx55737

Symptom Cisco Jabber Video for TelePresence (Movi) drops the call on CTS 3000 hold/resume.

Conditions This occurs when Movi is set to ForceTlsNoSrtp and the CTS is set to encrypted.

Workaround There is no workaround.

CSCtx38646

Symptom Scheduled static calls between the CTS and Polycom results in no presentation.

Conditions This occurs when a static point-to-multipoint call is manually dialed from the CTS. Polycom presentation is active from the CTS but fails to be seen on the Polycom.

Workaround Unshare and then share the presentation again.

CSCtx62312

Symptom Hold/Resume from the CTS shows frozen video from Cisco Jabber Video for TelePresence (Movi) for 10 seconds.

CSCtx41146

Symptom CTS calls Cisco Jabber Video for TelePresence (Movi) but there is no video on CTS after a hold/resume.

Conditions This occurs on both PC and Mac. The CTS is connected to Cisco Jabber (Movi) and a hold/resume on the CTS results in no video on the CTS. Cisco Jabber (Movi) is sending and receiving video resolution at 1280 X 720.

Workaround There is no workaround.

CSCtw50738

Symptom No video on the Cisco Roundtable (RT) phone 9971/9951/8961.

Conditions This occurs in a one way video call between the CTS and the RT phone over a secure SIP trunk. The call seems to be secure, showing the lock icon on both the RT and the CTS, but there is no video on the RT phone. This could be due to a Unified CM version mismatch if the remote endpoint does not support BFCP.

Workaround There is no workaround.

CSCtx38628

Symptom Polycom does not disconnect static non-secure calls.

Conditions Video freezes and the non-secure static call does not disconnect.

Workaround There is no workaround.

CSCtx17774

Symptom Calls can drop if a secure CTS does a hold/resume with non-secure endpoints/MCU.

Conditions .In CTS Release 1.7.4, it was helpful to do a media hold/resume to avoid interop issues with Cisco TelePresence Codec (TC4) software.

Workaround The release of the Cisco TelePresence Codec (TC5) solves the potential interop issues and there is no need to do a media hold/resume on the TC5.

CSCtu75116

Symptom CTS cannot share presentations with the Cisco E20 IP Video Phone.

Conditions The E20 does not support Rx BFCP presentation at 1024x768 resolution, so the SDP does not signal this capability and the presentation is not shared. This affects CTS software releases 1.7.4 and later releases.

Workaround There is no workaround.

CSCtx19741

Symptom Phones with mismatched load report incorrect for CTS endpoints.

Conditions Phones with Mismatched Loads Unified Report on Unified CM reports that CTS endpoints are not running the correct load when they are. Occurs for any CTS endpoints registered with Unified CM when attempting to view the Phones with Mismatched Loads Unified Report.

Workaround There is no workaround.

Resolved Caveats in CTS Release 1.8.1

CSCtu82870

Symptom Intermittent horizontal black bars at call start.

Conditions The bars disappear after 30-45 seconds. This occurs with CTS software release 1.7.4 and later releases.

Workaround End call immediately and call again or wait 30-45 seconds for the bars to disappear.

CSCtu07566

Symptom Directory hard button does not work.

Conditions When pressing the Directory button on the CTS Cisco Unified IP Phone, the following message appears: “Unable to connect to directory, please try again.” This can occur on any CTS running software release 1.7.x or higher when registered with Unified CM 8.6.2a. CTS Release 1.7.4 does not support Unified CM8.6.2.

Solution CTS Release 1.8.x now supports Unified CM 8.6.2.

Workaround Check that you are running compatible Unified CM firmware for your release. Use the Directory softkey on the phone instead of the Directory button on the touch pad.

CSCtu24513

Symptom Call drop due to system overload with unintended SSH session.

Conditions When the system is overload during a call, an unintended or runaway SSH session can occur due to lost control from remote user. This condition can contribute even more system load and impair the codec, causing abnormal function. For example, checkServices receive a timeout from subroutines resulting in a call drop.

Workaround Clean up runaway SSH sessions proactively to reduce the system overload.

CSCtv17399

Symptom No media received for secure call between CTS Release 1.7.2 and CTS Release 1.7.5.

Conditions When the call is in secure mode, the CTS display remains blank and logs report that no media was received on either side. When the same call is made in unsecured mode, the media flows as expected. Adding audio add-in made the call non-secure and the media started flowing.

Workaround Use non secure mode and audio add in to make calls between these two CTS software releases.

Caveats in CTS Release 1.8.0

- Unresolved Caveats in CTS Release 1.8.0, page 30
- Resolved Caveats in CTS Release 1.8.0, page 40

Unresolved Caveats in CTS Release 1.8.0

CSCty56195

Symptom CTS fails to register to CUCM when the CUCM cluster contains more than 4 nodes.

Conditions When inter-device security is enabled, the CTS can only cache four certificate entries in the CTL file. When the CTS tries to register a fifth CUCM node, it cannot cache the fifth certificate entry, and registration fails.

Workaround Contact Cisco TAC for a resolution to this issue.

CSCtw93670

Symptom Loss of camera status communication is seen after 22 days of system uptime.

Conditions The CTS 500-32 reports a camera error after 22 or more days of uptime. A similar issue occurs on the CTS 1300-47. This occurs on systems that use both the Cisco Unified IP Phone and the Cisco TelePresence Touch 12 call control devices. Systems that use the Cisco TelePresence Touch 12 cannot make calls and must be reset from Unified CM or power cycled. Systems using the Cisco Unified IP phone with MIDlets can still make calls, though camera status will show an error state.

Workaround Reset the CTS from the Unified CM administration or power cycle the device to clear the camera status error.

CSCtw45493

Symptom Mtg Ctrl softkey disappears after 2-3 minutes in a telepresence meeting.

Conditions The Mtg Ctrl softkey was no longer showing on the Cisco Unified IP phone two to three minutes after a meeting was started.

Workaround There is no workaround.

CSCtr92400

Symptom Encrypted CTS call may break after hold/resume with packet loss

Conditions Sometimes Datagram Transport Layer Security (DTLS) negotiation fails between the Cisco TelePresence Server and the CTS. Under some circumstances, media services are restarted if invalid video is sent to the CTS.

Workaround There is no workaround.

CSCtq70191

Symptom Call drops in a multipoint (CTMS) meeting after a hold/resume.

Conditions This occurred in CTMS Release 1.7.2(75) with the following Unified CM scenario in place for the call: 8.5 > 8.6 > 8.5 trunk in call.

Workaround End the call and call back.

CSCtt09629

Symptom Non-secure endpoints cannot connect to secure endpoints over SBC path.

Conditions The following message appears on the main display: “The call has been dropped because resources are not available” making a non-secure call from a non-secure endpoint to a secure endpoint over two different setups. When the same type of call is made without the Session Border Controller (SBC) or Cisco Unified Border Element (CUBE), the call goes through fine.

Workaround There is no workaround.

CSCtt22889

Symptom Unified CM (CUCM) 8.6 and session bandwidth issue in CTS-to-CTS call.

Conditions Media level bandwidth for video line and content line are the same for calls. Even if remote indicates the content line should have lesser bandwidth. Point-to-Point call with CTS, where CTS advertises lower presentation media bandwidth.

Workaround There is no workaround.

CSCts33202

Symptom Media services restart while hold resume on Cisco TelePresence TS4

Conditions Sometimes hold and resume reaction is slow and media service restarts on the Cisco TelePresence TS4 when the Cisco TelePresence TS4 calls the Cisco TelePresence Movi PC (set to 800x600). This occurs with Unified CM 8.6.

Workaround There is no workaround.

CSCto71973

Symptom Call “on-hold” message is displayed on the Cisco TelePresence E20 after a hold/resume.

Conditions Message on the Cisco TelePresence E20 “Your call put on hold” is displayed even after resuming the call.

Workaround There is no workaround.

CSCtq44109

Symptom Video sent by a Cisco MXP 3000 to the CTS is pixelated in P2P call.

Conditions The CTS image is 1.7.4(201) running Unified CM version 8.5.1 and is registered to the Cisco Video Communications Server (VCS).

Workaround There is no workaround.

CSCtq44157

Symptom Cisco MXP 3000 does not renegotiate call rate when new a participant joins.

Conditions Possibly due to legacy H.323 and H.320 implementation. The CTS image is 1.7.4(201) running Unified CM version 8.5.1.

Workaround There is no workaround.

CSCtu24860

Symptom Black screen seen on CTS during a security/resolution downgrade.

Conditions This occurs when multiple hold/resumes are performed on the CTS after it calls the TAA endpoint and shares a Presentation. After a hold/resume on the CTS black screens appear (if presentation source connected, then it displays local presentation in between) and then shows the main Video.

Workaround There is no workaround.

CSCts29266

Symptom Cisco TelePresence Movi call only has one-way video.

Conditions Sometimes when Cisco VCS is involved in the call, there is a possibility of receiving one-way video. This occurs in VCS deployments when UCM sends the re-invite for security status updates, or session timer refresh.

Workaround There is no workaround.

CSCtn40939

Symptom CTS calls a Cisco MXP 1000 with SCCP poor video quality seen in Cisco MXP after a hold/resume.

Conditions The CTS calls a Cisco TelePresence System 1000 MXP with SCCP and delayed or stuck video is seen on the Cisco TelePresence System 1000 MXP after a hold/resume.

Workaround There is no workaround.

CSCtn50573

Symptom Cisco TelePresence System 1000 MXP with SCCP: No audio on the Cisco TelePresence System 1000 MXP after an audio addin.

Conditions An issue with SCCP on the Cisco TelePresence System 1000 MXP causes a delay in resuming a call after audio addin; eventually audio/video between the CTS and Cisco TelePresence System 1000 MXP is established.

Workaround Increase the volume on the Cisco TelePresence System 1000 MXP to hear the audio.

CSCtu25166

Symptom SIP messages are not shown in Administration logs.

Conditions When troubleshooting using Troubleshooting > Log Files > SIP Messages, the messages truncate and do not list properly.

Workaround There is no workaround.

CSCtr15284

Symptom Video received from the Cisco TelePresence MXP to the CTS was corrupted.

Conditions The video image is corrupted in SIP calls from the CTS 1300 to the Cisco TelePresence 1700 MXP. Unsupported video resolution received from remote end point, intermittent blank screen, and the muted microphone icon is not shown.

Workaround There is no workaround.

CSCts19075

Symptom Local presentation (PiP) shared in a call with the Cisco TelePresence C90 when calls go on hold.

Conditions This occurs before plugging in the VGA cable. Presentation alert is shown on the phone when “Just me” is selected and local view (PiP) shows frozen video on the CTS.

Workaround This is expected behavior between the Cisco TelePresence C90 and the CTS 500-32. The hold function takes a few seconds to process.

CSCts27500

Symptom Some CTS 1300 systems cannot make secure calls.

Conditions This only occurs in the One Phone per Office feature setup (phone directly connected to the network). When the phone is only connected to the codec and not the network, the issue is not seen and secure calls can be made.

Workaround There is no workaround.

CSCts47288

Symptom Video freezes on Cisco TelePresence Movi PC in Presentation mode.

Conditions This occurs during a presentation share from the CTS to the Cisco TelePresence TS4 endpoint when the hold/resume function is used.

Workaround There is no workaround.

CSCts68292

Symptom Unplugging the presentation and plugging back on some CTS 1300s shows Blue PiP.

Conditions Blue PiP shows on the remote side.

Workaround Unplug the presentation cable and plug it back in.

CSCts80076

Symptom Call drops after audio addin in a secure interop call.

Conditions This occurs on a secure call on a Cisco TelePresence Ex90. After conferencing in a non-secure audio addin, the call drops.

Workaround There is no workaround.

CSCts96560

Symptom SNMP supports on BFCP

Conditions There is no BFCP support on the call MIB. The MIB should show the media port number and the corresponding presentation statistics.

Workaround There is no workaround.

CSCtt15735

Symptom On between a Non-secure Cisco Movi and a secure CTS, Cisco Movi denies the call after a CTS Hold/Resume.

Conditions When the call disconnects from Cisco Movi, the following message appears: “Your call was denied due to mismatching encryption settings.”

Workaround There is now workaround.

CSCtt19841

Symptom Audio addin fails if there is a Unified CM TCP connection failure.

Conditions The connection is closed by Unified CM.

Workaround There is no workaround. Disconnect all the calls to try again.

CSCtt35671

Symptom No audio and “Remote user on-hold” message shown on CTS after a hold/resume.

Conditions This occurs between the CTS and a Cisco Unified IP 9971 Round Table phone. Remote user on-hold message is displayed on the CTS and no audio is heard on either side.

Workaround There is no workaround.

CSCtt36038

Symptom Cisco Movi showing frozen screen on calls with CTS 3000.

Conditions Once the call connects, Cisco Movi shows a frozen screen for about 1 to 2 minutes and then recovers.

Workaround There is no workaround. Wait for the screen to recover.

CSCtu07566

Symptom Directory hard button does not work.

Conditions When pressing the Directory button on the CTS Cisco Unified IP Phone, the following message appears: “Unable to connect to directory, please try again.” This can occur on any CTS running software release 1.7.x or higher.

Workaround Check that you are running compatible Unified CM firmware for your release. Use the Directory softkey on the phone instead of the Directory button on the touch pad.

Resolved in CTS Release 1.8.1.

CSCtu08086

Symptom Document camera presentation shows black PiP during recording playback.

Conditions After recording and saving the video with “record presentation” option enabled, black PiP is shown upon playback.

Workaround There is no workaround.

CSCtu10328

Symptom Receiver reports sent with incorrect key in secure call with the Cisco TelePresence EX90.

Workaround There is no workaround.

CSCtu10835

Symptom Cisco MXP 6000 codec has a frozen screen after the document camera powers on/off while sharing a presentation.

Conditions This occurred when attempting to turn the document camera off. Instead of the Cisco MXP screen going black, it froze.

Workaround There is no workaround.

CSCtu19709

Symptom Digital media player: Outside of business hours video switches off after 10 minute timeout.

Conditions After business hours if you turn on the DMP, no audio is heard, video displays but then times out. The DMP should remain turned on if user has turned it on manually.

Workaround There is no workaround.

CSCto89367

Symptom CTS-CUVC conference dropped after CTS hold-resume with Unified CM 8.0.

Conditions CTS will drop a CUVC call after hold/resume when using Unified CM 8.0.

Workaround Upgrade to Unified CM release 8.5.

CSCts06855

Symptom Cisco TelePresence C90 PC audio heard when CTS overrides with its presentation.

Conditions Video of the CTS presentation is played.The audio from Cisco TelePresence C60 presentation as well as CTS PiP presentation is played.

Workaround On the C series endpoint, navigate to and change the MuteOnInactiveVideo configuration as follows:

Advanced Configuration > Input > Microphone 1 > Video Association > MuteOnInactiveVideo: ON

Make sure to associate to the correct Video Input Source. Alternately, to disable audio when an associated video input is not active, set the Audio Input Microphone 1 VideoAssociation MuteOnInactiveVideo to off.

CSCts64918

Symptom Video Bit rate shows “NULL” when configuring “Limited BW: 360p” for CTS Release 1.7.4.

Conditions When configuring Quality (per Display) in the Unified CM Administration.

Workaround Limited bandwidth mode: 360p may be listed as an option in the Quality (per Display) field in the Unified CM Administration but is not yet available; it is supported in a future release.

CSCtu19775

Symptom Document camera power button goes out of sync when the CTS is rebooted.

Conditions After the CTS reboots, and you tap the Doc Cam button to launch the document camera control screen, the Power On button is displayed in the application instead of the Power Off button. The Power Off and document camera control buttons should be visible.

Workaround Tap the Power button to resync the control buttons.

CSCts68355

Symptom CTS version 1.7.4 support and SDP/SRTP.

Conditions Newly added “multiple crypto attributes” are blocked by SBC and do not allow multiple crypto attributes in an SDP.

Workaround Use the SDP edit feature. See SDP and SRTP with CTS Release 1.7.4 and CTS Release 1.8.0.

CSCtn24147

Symptom SSCD does not report peripheral status and SNMP polling fails.

Conditions Randomly the administration interface peripheral status shows a red X but there is no other functional impact.

Workaround Reboot the codec.

CSCtr49077

Symptom Cisco Unified IP Phone MIDlet does not handle incoming call while playback or recording.

Conditions When there is an incoming call during recording or playback, the user can opt to continue with the recording or playback, but the incoming call ring continues until it reaches the configured timeout. You can press **Stop** or **Exit** while recording or playback to accept the call, but the call may not go through.

Workaround Ignore the incoming call or discontinue the call from the other end or from the handset to restore the system for recording or playback.

Resolved Caveats in CTS Release 1.8.0

There are no known resolved caveats in this release.

Caveats in Cisco TelePresence Touch 12

See the following sections for information about unexpected behavior found on the Cisco TelePresence Touch 12 in the CTS Release 1.8 releases:

- Caveats in CTS Release 1.8.0, page 40
- Caveats in CTS Release 1.8.1, page 40

Caveats in CTS Release 1.8.1

- Cisco TelePresence Touch 12 Unresolved Caveats in CTS Release 1.8.1, page 40
- Cisco TelePresence Touch 12 Resolved Caveats in CTS Release 1.8.1, page 40

Cisco TelePresence Touch 12 Unresolved Caveats in CTS Release 1.8.1

There are no known unresolved caveats in this release.

Cisco TelePresence Touch 12 Resolved Caveats in CTS Release 1.8.1

There are no known resolved caveats in this release.

Caveats in CTS Release 1.8.0

- Cisco TelePresence Touch 12 Unresolved Caveats in CTS Release 1.8.0, page 40
- Cisco TelePresence Touch 12 Resolved Caveats in CTS Release 1.8.0, page 45

Cisco TelePresence Touch 12 Unresolved Caveats in CTS Release 1.8.0

CSCtu00932

Symptom Cisco TelePresence Touch 12 UI displays register and unregister from Unified CM alert.

Conditions The “Not registered” alert is displayed on the touch screen but the call is not disconnected.

Workaround There is no workaround. Press the Answer/End call hard button on the Cisco TelePresence Touch 12 console to end the call.

CSCts43318

Symptom Cisco TelePresence Touch 12 displays “system issue” instead of “camera issue.”

Conditions The system issues a message when the camera is unplugged: “Telepresence calls are not possible at this time. Please contact your system administrator for assistance.” The message should be: “Camera Issue - Telepresence calls are not possible at this time. Please contact your system administrator for assistance.”

Workaround There is no workaround. This is a cosmetic issue that does not affect functionality.

CSCtu28325

Symptom “Establishing connection to codec” displayed on Cisco TelePresence Touch 12 after UI crash.

Conditions This message appears during a memory crash, active calls are removed from the UI, and a the DN is not displayed. The system recovers in about 30 seconds and the idle display window appears first, followed by the active call window.

Workaround There is no workaround.

CSCtu04961

Symptom Directory stuck in “loading” animation scrolling.

Conditions The loading animation persists for approximately 20 seconds while scrolling through the Directory search then disappears.

Workaround There is no workaround.

CSCts56824

Symptom Black PiP window on remote endpoint during local video refresh in a point-2-point call.

Conditions This sometimes occurs on calls between two CTS 500-32, when you choose “everyone” for presentation sharing option and while the document camera is powered off.

Workaround There is no workaround.

CSCtu07975

Symptom Recording stuck in “connecting” screen while recording CIF recording.

With the max number of recordings set to 3, after tapping Record, the touch screen displays “Connecting” while the CTS main display shows video and timer count.

Workaround There is no workaround.

CSCtu07956

Symptom On-screen display (OSD) does not turn off after user is unable to record.

Conditions Self view does not end when recording fails to start while system is at the maximum number of callers. The following alert is displayed on the Cisco TelePresence Touch 12: “System is at maximum number of callers.” Recording does not start and the touch screen returns to the recording list screen.

Workaround Wait approximately 30 seconds for the user interface to refresh.

CSCtt94368

Symptom Cisco TelePresence Touch 12 screen frozen for about 30 seconds and then accessible again.

Conditions Occasionally the touch screen freezes from too many taps too quickly. The “establishing connection to the codec” message may be seen.

Workaround Wait approximately 30 seconds for the screen to refresh.

CSCtu07821

Symptom Cisco TelePresence Touch 12 installation bootup is stuck on Step 4 and the message “Unable to communicate with the codec” is seen.

Conditions Access switchport is configured with the same voice and access VLANs.

Workaround Configure separate voice and access VLANs.

CSCtt93919

Symptom CTS to be reset when you swap document cameras running different firmware.

Conditions Then the document camera was swapped with another document camera running different firmware and some of the menu buttons that operate the document camera were not displayed on the Cisco TelePresence Touch 12. This is seen on CTS with both the Cisco TelePresence Touch 12 and the Cisco Unified IP phone.

Workaround Make sure that a document camera has been configured for your system by your administrator. Reset the CTS so that the new camera is discovered correctly so that all the menu buttons are available.

CSCtr72983

Symptom DMP audio cannot be heard outside of business hours.

Conditions The Cisco TelePresence Touch 12 currently does not allow the DMP to be used after business hours.

Workaround There is no workaround.

CSCts09587

Symptom Document camera status shows a question mark (?).

Conditions The Document camera is connected and the presentation can be seen locally and remotely, but the document camera status entry in System Status > Peripherals displays a question mark.

Workaround The document camera is not configured in Unified CM. Configure the document camera.

CSCtu00932

Symptom Cisco TelePresence Touch 12 UI displays register and unregister from Unified CM alert.

Conditions The “Not registered” alert is displayed on the touch screen but the call is not disconnected.

Workaround There is no workaround. Press the Answer/End call hard button on the Cisco TelePresence Touch 12 console to end the call.

CSCtt19925

Symptom Available time is not displayed on the UI if the Cisco TelePresence Touch 12 is rebooted after 23:00 PM.

Conditions After 23:00 PM, if the Cisco TelePresence Touch 12 or the CTS is rebooted, the Calender "Available Time" header is empty and the Calendar screen is blank until 24:00 if there are no scheduled meetings. If a new meeting is scheduled during that time after reboot, it will appear on the Calendar as expected.

Workaround This is expected behavior.

CSCtu19529

Symptom "Connection lost" message is displayed on Cisco TelePresence Touch 12 after user starts/stops recording.

Conditions An unexpected message is seen after you tap the Stop button immediately after starting a recording. The connection is restored after about one minute; any recording that had been started is lost and you cannot record while you are disconnected.

Workaround There is no workaround.

CSCts10775

Symptom The In-call screen animation displays shift before being set in foreground.

Conditions The In-call screen animation displays a horizontal positioning shift on Touch 12 for a split second before settling in the foreground as expected. This happens when a call is dialed.

Workaround The call dials as expected. This is a cosmetic issue that does not affect functionality.

CSCtw47775

Symptom Selecting "Ignore" for an incoming call ends self view.

Conditions Self view is on and there is an incoming call. If user taps **Ignore** on the incoming call popup dialog, self view is turned off. Self view should display until it times out or **Exit** is tapped to manually end self view.

Workaround Restart self view.

Cisco TelePresence Touch 12 Resolved Caveats in CTS Release 1.8.0

There are no known resolved caveats in this release.

Caveats in Prior CTS Releases

See the Cisco TelePresence Administration Software Release Notes home page on Cisco.com for information about prior CTS releases:

http://www.cisco.com/en/US/products/ps8332/prod_release_notes_list.html

Supported CTS Auxiliary Devices

This section contains auxiliary devices that can be used with the Cisco TelePresence System:

Displays

Cisco TelePresence systems are designed to work with any Full HD monitor that connects to the system using a standard HDMI or DVI interface. Note that the connector on the TelePresence side is an HDMI connector, so either an HDMI-to-HDMI cable or an HDMI-to-DVI cable is required.

Cisco highly recommends the use of commercial or professional-grade displays with your Immersive TelePresence system. Off-the-shelf consumer displays or TV monitors are not recommended, as they typically have shorter life spans and require a remote control to operate.

When qualifying a display for use with your TelePresence system, consider the following:

- The display should offer native support for 1080p60 over an HDMI or DVI interface.
- The display should become active when a video signal is presented, and should go to sleep when no video signal is presented.
- The display should not require any user interaction (such as a remote control or button press) to become active from standby, sleep or deep sleep modes.
- The ability to switch off On-Screen Display (OSD) messages is highly desirable. No error messages, status messages or splash screens should be visible on the screen when a presentation image is shared or unshared.
- If the display supports multiple inputs, the ability to lock the display to a given input is highly desirable. Otherwise, the time required to show presentation content can be unpredictable. If automatic scanning of ports is supported, the feature should be disabled.

Document Cameras

The following WolfVision document cameras have been tested for use with Cisco TelePresence Systems:

- VZ-C12 (Ceiling mounted)
- VZ-C32 (Ceiling mounted)
- VZ-C32[3] (Third Generation product line)
- VZ-9plus (Desktop unit)
- VZ-12[3] (All)

Projectors

The following projectors are supported:

- Sanyo PLV-Z60—CTS 3000 and CTS 3200 systems.
- Sanyo PLV-Z700—CTS 3000 and CTS 3200 systems.

Note Cisco maintains support for the Sanyo PLV-Z4 and Sanyo PLV-Z5 projector models in older CTS configurations.

Video Signal Splitters

The following video signal splitters have been tested for use with the CTS:

- GEFEN EXT-HDMI-144
- EXT-HDMI-144-BLK
- GEFEN EXT-HDMI1.3-144
- GEFEN GTV-HDMI1.3-144

Note **Using External Devices with Your Cisco TelePresence System**—Cisco cannot guarantee the performance of any external device, so Cisco recommends that you choose good quality external devices to optimize CTS performance.

The CTS works best when suitable devices are attached using good quality cables and connectors. Cisco does not supply the cable that connects auxiliary devices to the codec.

Caution In European Union countries, use only devices that are fully compliant with the EMC Directive [2004/108/EC].

For information about managing video signal splitters, see the Routing Power and Signal Cables chapters of the following guides on Cisco.com:

- Cisco TelePresence System 3000 Assembly, Use & Care, and Field-Replaceable Unit Guide
- Cisco TelePresence System 3200 Assembly, Use & Care, and Field-Replaceable Unit Guide

Software Agreements and Licensing

For complete software licensing information, access the Cisco TelePresence Administration Software Licensing Information page on Cisco.com at the following link:

http://www.cisco.com/en/US/products/ps8332/products_licensing_information_listing.html

Related Documents

Related Topic	Document Title
Software Documents	
How to configure, troubleshoot, and maintain the CTS using the administration Web interface.	• *Cisco TelePresence System Administration Guide* home page on Cisco.com.
Cisco command-line interface (CLI) information for configuring the Cisco TelePresence System.	• *Cisco TelePresence System Command-Line Interface Reference Guide*.
Cisco TelePresence Administration Software Compatibility Information.	• Cisco TelePresence Software Compatibility Matrix
How to troubleshoot the Cisco TelePresence System.	• *Cisco TelePresence System Troubleshooting Guide*
Cisco Unified CM configuration with the Cisco TelePresence System.	• *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
Cisco Unified Communications Manager Support page.	• Cisco Unified Communications Manager Support
How to use the Cisco TelePresence System, including the CTS Cisco Unified IP Phone.	• *Cisco TelePresence System User Guide*
Cisco TelePresence Touch 12 home page.	• Cisco TelePresence Touch
Cisco Unified IP Phones 7900 Series documentation.	• Cisco Unified IP Phones 7900 Series Maintain and Operate Guides
Cisco TelePresence System (CTS) hardware and software documentation, including information about CTS devices.	• Cisco.com **Products > TelePresence > Cisco TelePresence System > TelePresence System**
Cisco TelePresence Administration Software documentation and software download page.	• Cisco TelePresence Administration Software
Roadmap of Cisco TelePresence System (CTS) hardware and software installation and configuration documents, including guides to install and operate optional software applications.	• Cisco TelePresence Administration Software Documentation Roadmaps
How to locate software features for your Cisco TelePresence System device and supporting peripherals.	• *Cisco TelePresence System Software Feature Guide*
Cisco TelePresence Manager documentation home page.	• Cisco TelePresence Manager
Cisco TelePresence Multipoint Switch home page.	• Cisco TelePresence Multipoint Switch

Cisco TelePresence Recording Server information.	• Cisco TelePresence Recording Server
Cisco TelePresence System system message information.	• Cisco TelePresence System Message Guide
Cisco Validated Design Program. Systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments.	• *Cisco TelePresence Network Systems 2.0 Design Guide*
Session Initiation Protocol (SIP) page.	• Session Initiation Protocol (SIP)
Cisco Unified IP Phone 8900 Series home page.	• Cisco Unified IP Phone 8900 Series
Cisco Unified IP Phone 9900 Series home page.	• Cisco Unified IP Phones 9900 Series
Cisco TelePresence System Codec home page.	• Cisco Telepresence System Integrator C Series
Cisco TelePresence System EX Series home page.	• Cisco TelePresence System EX Series
Cisco TelePresence Video Communication Server (VCS) home page.	• Cisco TelePresence Video Communication Server (VCS)
Cisco TelePresence Movi home page.	• Cisco TelePresence Movi
Information about SNMP in Cisco product solutions.	• Simple Network Management Protocol (SNMP)
Cisco TelePresence System MXP Series home page.	• Cisco TelePresence System MXP Series

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.