Cisco TelePresence System Administration Guide

April 2013
CTS Software Release 1.10

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-28614-01

Cisco TelePresence System Administration Guide

What's in This Guide

April 2013, OL-28614-01

What's New

For a complete list of features for this release, see the following documentation on Cisco.com:

- *Release Notes for Cisco TelePresence System*

For supported software compatibility across all releases, see the following documentation:

- Cisco TelePresence Administration Software Compatibility

Before You Begin

Before beginning the tasks in this guide, familiarize yourself with the following:

Call Control Device Information

Cisco TelePresence Touch 12 Requirements

See the Installing and Configuring the Cisco TelePresence Touch 12 on Cisco.com.

Cisco Unified IP Phone Requirements

Each Cisco TelePresence/IP phone combination takes 11 units of the Unified CM unit license:

- 5 units for the Cisco Unified IP Phone 7970/7975
- 6 units for the Cisco TelePresence unit.
- CTS and the Cisco Unified IP Phone are both configured in Unified CM as a shared line.

Note 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.

Configure the Cisco Unified IP phone as follows:

1. If option 150 of DHCP is enabled—**Alternative TFTP=NO**
2. If you use manual entry—**Alternative TFTP=YES**

   For more information about the Cisco Unified IP Phone 7970/7975 series, refer to the Cisco Unified IP Phones 7900 Series Maintain and Operate Guides page at the following URL: http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

CTS Assembly and Wiring Guidelines

Make sure your CTS is properly assembled and wired according to the guidelines in the Cisco TelePresence System assembly documentation. See the Cisco TelePresence System Install and Upgrade Guides for your system on Cisco.com by navigating to cisco.com, clicking **Support**, and entering the name of your product.

CTS Software Download Support

Make sure you have downloaded supported CTS software. Navigate to your CTS device on Cisco.com.

Step 1 Navigate to your device:

- **Product Support > TelePresence > TelePresence Immersive Endpoints**
  - Cisco TelePresence System 3200 Series

- Cisco TelePresence System 3000 Series
- Cisco TelePresence System 1300 Series

- **Products > TelePresence > TelePresence Personal Endpoints > TelePresence Office**
  - Cisco TelePresence System 1100
  - Cisco TelePresence System 1000
  - Cisco TelePresence System 500-37

For example:

Products > TelePresence > TelePresence Endpoints - Immersive > Cisco TelePresence System 1300 Series > Cisco TelePresence System 1300-65 > TelePresence Software-1.9.1.1(2)

Step 2 Select software and choose whether to download now or add it to your cart. For example:

Description: Cisco TelePresence System Software for CTS500, CTS1000, CTS1100, CTS1300, CTS3000, CTS3010, CTS3200 and CTS3210

Release: 1.9.3(44)

Release Date: 04/Dec/2012

File Name: cmterm-CTS.1-9-3-44R-K9.P1.cop.sgn

Size: 88.93 MB (93245986 bytes)

DHCP Connectivity Requirements

Provide a Dynamic Host Configuration Protocol (DHCP) server to achieve connectivity. CTS uses DHCP by default. You can, however, configure a system that does not use DHCP with a static IP address; to do so, see the "Configuring a Static IP Address for Networks That Do Not Use DHCP" section on page 4.

Laptop Screen Resolution Recommendation

For best results, Cisco recommends that you change your laptop screen resolution to 1024 x 768.

MAC Address Availability

Make sure the MAC address of the device you are installing is known or available:

- The MAC address comprises a unique 12-character hexadecimal number that identifies a Cisco Unified IP phone or other hardware device.
- Locate the MAC address number on a label on the back of the Cisco TelePresence system primary codec (for example, 000B6A409C405). Unified CM makes the MAC address a required field for Cisco Unified IP phone device configuration.

  The MAC address is also displayed on the CTS main display screen during boot-up.

Note When entering the MAC address in Unified CM fields, do not use spaces or dashes, and do not include any other characters that may precede the MAC address on the label.

Network Time Protocol (NTP) Requirements

NTP is required to synchronize the clocks on Cisco IP telephony servers. NTP must be configured properly to ensure that calendar events appear as expected.

See Table 4-5 in Chapter 4, "Configuring the Cisco TelePresence System" for more information about configuring NTP and other CTS system settings.

Unified Communications Manager and MIDlets Download Support

Make sure that Unified CM is running and is using supported software for your release. 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

Note If your system uses a Cisco Unified IP Phone for call control, you must download and configure MIDlets. The supported MIDlet version is embedded in the software files that are available when you click Download Software on the Cisco Unified Communications Manager Support page at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Or navigate to **Products > Voice and Unified Communications > IP Telephony > Call Control > Cisco Unified Communications Manager (CallManager) > Cisco Unified Communications Manager Version x.x > Unified Communications Manager/CallManager Device Packages**.

Check the following:

- The Cisco TelePresence device name in Cisco Unified CM follows the following format: The characters "SEP" followed by the device MAC address. Assign the hostname so that it is resolvable by Domain Name System (DNS), for example:

  MAC address: " **00:0D:D1:23:45:A1** "

  Cisco TelePresence Host Name: " **SEP000DD12345A1** "

Note DNS (domain) is optional.

Unified Communications Manager and COP File Download Support

See Managing Cisco Options Package (COP) Files on the Cisco TelePresence System in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Web Browser Support

The Cisco TelePresence System Administration interface is supported on Internet Explorer (IE) versions 8 and 9, as well as the latest version of Firefox.

Document Organization

Information about using the Cisco TelePresence System Administration interface is provided in the following chapters:

- Chapter 1, "Using the Cisco TelePresence System Administration Interface"
- Chapter 3, "Device Information"
- Chapter 4, "Configuring the Cisco TelePresence System"
- Chapter 5, "Monitoring the Cisco TelePresence System"
- Appendix 6, "Satellite Licenses for the Cisco TelePresence System"
- Glossary
- Index

Related Documents

Document Title	Related Topic
• Cisco Digital Media Players	Digital Media Player home page on Cisco.com.
• Cisco TelePresence Administration Software Release Notes home page on Cisco.com	Cisco TelePresence System (CTS) Release Notes. Describes new features and open and closed hardware and software caveats for software releases.
• Installation Notes section of the *Cisco Unified IP Phone Release Notes for Firmware Release 8.5(3) (SCCP and SIP)*	Cisco Unified IP Phone firmware download instructions.
• Cisco TelePresence Administration Software Command References home page on Cisco.com	Cisco command-line interface (CLI) information for configuring the Cisco TelePresence System.
• Cisco TelePresence Administration Software End-User Guides on Cisco.com	Cisco TelePresence User Guide and Quick Reference Card, including information about using the CTS Cisco Unified IP phone.
• Cisco TelePresence Administration Software Troubleshooting Guide	Troubleshooting the Cisco TelePresence System, including Unified CM administration and CTS Cisco Unified IP phone issues.
• Cisco TelePresence Manager home page on Cisco.com	Cisco TelePresence Manager documentation home page.
• Cisco TelePresence MCU 4500 Series	Cisco Multipoint Control Unit (MCU) 4500 Series home page.
• Cisco Jabber for TelePresence	Cisco Jabber for TelePresence (Movi) home page.
• Cisco TelePresence Multipoint Switch	Cisco TelePresence Multipoint Switch (CTMS) home page on Cisco.com.
• Cisco TelePresence Recording Server home page on Cisco.com	Cisco TelePresence Recording Server information.
• *Cisco TelePresence Security Solutions*	Configuring security in Cisco TelePresence systems.

• *Cisco TelePresence System Documentation Roadmap*	CTS software and hardware documentation roadmap.
• Cisco TelePresence System EX Series	Cisco TelePresence System EX Series home page.
• Cisco Telepresence System Integrator C Series	Cisco TelePresence System Codec home page.
• *Cisco TelePresence System Message Guide*	Cisco TelePresence System system message information.
• Cisco TelePresence System MXP Series	Cisco TelePresence System MXP Series home page.
• Cisco Unified Communications Manager (CallManager) Documentation Roadmaps	Unified CM support documentation.
• *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*	Cisco Unified CM installation with the Cisco TelePresence System.
• Cisco Unified Communications Manager Support	Cisco Unified Communications Manager Support page.
• *Cisco Unified Communications Manager with Cisco VCS Cisco TelePresence Deployment Guide* • *Cisco TelePresence Video Communication Server (VCS)*	Cisco TelePresence Video Communication Server (VCS) support documentation
• Cisco Unified IP Phone 8900 Series	Cisco Unified IP Phone 8900 Series documentation.
• Cisco Unified IP Phone 8900 Series	Cisco Unified IP Phone 8900 Series home page.
• Cisco Unified IP Phones 7900 Series Maintain and Operate Guides	Cisco Unified IP Phones 7900 Series documentation.
• Cisco Unified IP Phones 9900 Series	Cisco Unified IP Phone 9900 Series home page.
• Download Software Select a Product page on Cisco.com: http://www.cisco.com/cisco/software/navigator.html	Cisco TelePresence administration software download page.
• *Installing and Configuring the Cisco TelePresence Touch 12* • *Cisco TelePresence Touch 12 User Guide* • *Cisco TelePresence Touch 12 Meeting Quick Reference*	Install and use the Cisco TelePresence Touch 12.

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 the following URL:

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.

Using the Cisco TelePresence System Administration Interface

Created: April 2013, OL-28614-01

Contents

This chapter contains the following sections:

Overview

Administrators use the Cisco TelePresence System Administration interface to maintain the Cisco TelePresence System (CTS).

Note No more than one administrator should access the CTS Administration interface at one time.

Administration tasks include the following:

- Viewing device information and detailed system status information
- Configuring system settings
- Monitoring the status of Cisco TelePresence system equipment
- Troubleshooting the system

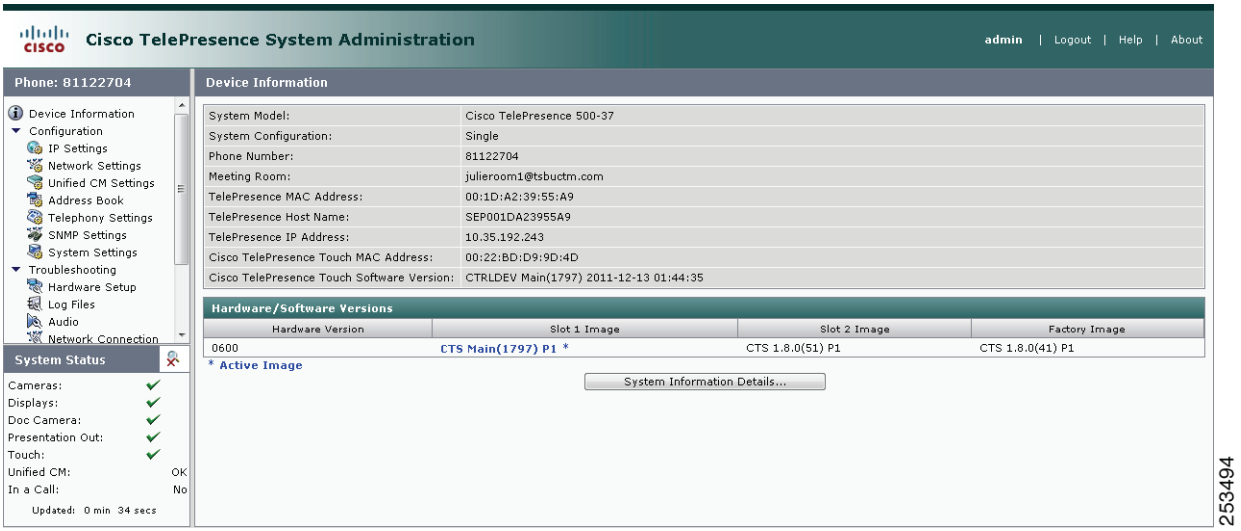
For first-time setup instructions, refer to the Cisco TelePresence System Assembly Guide for your system on Cisco.com:

- **Product Support > TelePresence > TelePresence Immersive Endpoints**

  - Cisco TelePresence System 3200 Series
  - Cisco TelePresence System 3000 Series
  - Cisco TelePresence System 1300 Series
- **Products > TelePresence > TelePresence Personal Endpoints > TelePresence Office**
  - Cisco TelePresence System 1100
  - Cisco TelePresence System 1000
  - Cisco TelePresence System 500-37

Figure 1-1 shows an example of the Cisco TelePresence System Administration window. Click the task name or the arrows in the left panel to navigate to tasks.

Figure 1-1 Main Cisco TelePresence System Administration Window



System Status

This section contains the following system status information:

- System Status Window, page 1-3
- Device Status Indicators, page 1-4
- Cisco Unified Communications Manager Status, page 1-5
- In a Call Indicator, page 1-5

System Status Window

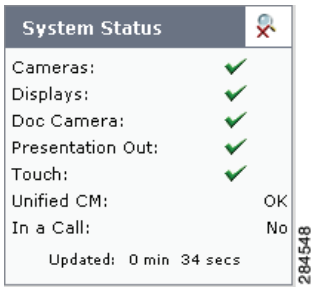
System status is always in view in the lower left corner of the Cisco TelePresence System Administration screen, as shown in Figure 1-2. The system administrator should closely monitor this area for changes in the status of the Cisco TelePresence system functions and equipment. The system status is updated every 60 seconds.

Note Information provided in the System Information Details window is used by Cisco technical support personnel to assist in troubleshooting your system.

To view detailed status information in the System Status box:

Step 1 Move your mouse over the colored icons in the System Status box to display dialog boxes containing the state of each piece of equipment. For example, rolling your mouse over the green check-mark icons in Figure 1-2 will show the detailed state of the equipment.

Figure 1-2 System Status Window



Or

Step 2 Click the magnifying glass icon in the upper right corner of the System Status box. A new window opens with the following two tabs:

- **System Information Details**—Lists detailed information about your CTS, including the camera, audio, and display.
- **Status Details**—Lists status details of CTS components and software, including the camera, presentation display, the Presentation Codec, and whether your Unified CM configuration is enabled and OK.

For more information, see Chapter 3, "Device Information."

Device Status Indicators

CTS devices include the following:

- Cameras
- Displays
- Document Camera
- Presentation display
- Room IP Phone

The System Status box shows the following icons for the camera, display, documentation camera, presentation display, and room IP phone for the conditions indicated.

- Ellipses or Black Dot—Microphone is not expected or microphone is not connected.

- Green check mark—Device is configured and operational.

- Hourglass—Device status is unknown or is being determined.

- Question Mark—Microphone is not expected or microphone is not connected.

- Red X with a broken pipe—Device in inaccessible. This icon is seen if the primary codec cannot communicate with a secondary codec.

- Red X—Device is not connected or device is not configured:
  - Cameras—When the video cable is not connected or is loose, or when the Ethernet cable is not connected.
  - Displays—When the video cable is not connected or the display does not have power.
  - Presentation displays—If the video cable is unplugged or the unit does not have power.
  - Microphones—Offline.
  - If you have specified in Cisco Unified Communications Manager (Unified CM) that a presentation display is present and there is not one present.

Determining Device Status Using the Troubleshooting Interface

To determine individual microphone and speaker functionality, use the hardware troubleshooting interface for your system. Refer to the "First-Time Setup" chapter for your Cisco TelePresence System to run testing procedures for each of your system components:

- *Cisco TelePresence System 500-37 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence 1000 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 1100 Assembly, First-Time Setup, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 1300-65 Assembly, First-Time Setup, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3000 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3010 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3200 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3210 Assembly, Use & Care, and Field-Replaceable Unit Guide*

Also see the "Troubleshooting Tabs" section on page 1-8 for information about updates to the CTS Administration troubleshooting interface.

Cisco Unified Communications Manager Status

The Cisco Unified Communications Manager can be in the following states:

- Enabled and OK
- Inaccessible

In a Call Indicator

The Status box tracks when the meeting room is in a call and displays the security level of active calls. When in a call, the security level is determined between the two endpoints. There are five possible levels of levels of security.

- **Yes/Encrypted**—Active call with both the signaling and the media encrypted.
- **Yes/Authenticated**—Active call with encryption on the call signaling only.
- **Yes/Non-Secure**—Active call with no authentication or encryption.
- **Yes/Not Available**—Active call but the security level of that call is unavailable.
- **No**—Not actively in a call.

Navigation

In the navigation pane at the left side of the Cisco TelePresence System Administration window, the Configuration, Troubleshooting, and Monitoring folders display lists of tasks. Lists of tasks are also displayed in the main content area of the window when you click any of the following topics in the navigation pane:

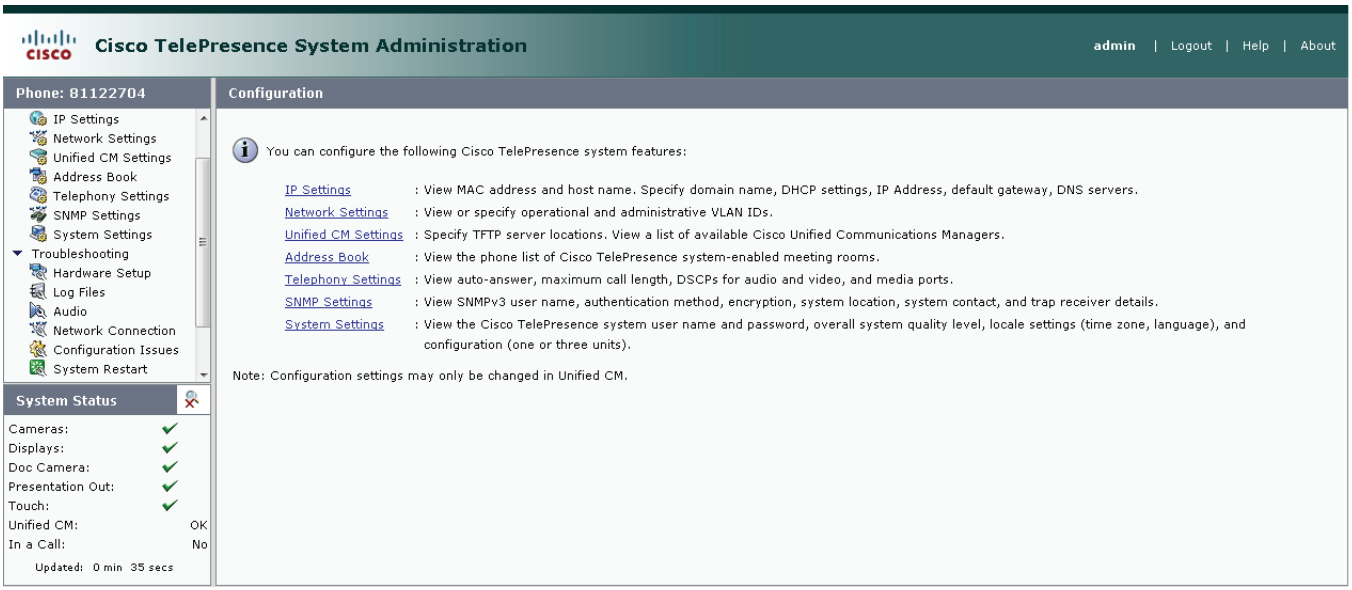
- Configuration
- Troubleshooting

- Monitoring

You can quickly access a task by clicking the highlighted name (IP Settings, for example).

Figure 1-3 shows your choices for accessing system administration tasks.

Figure 1-3 Choosing Cisco TelePresence System Administration Tasks



The following sections describe objects, functions, and information that is displayed in the windows associated with the Cisco TelePresence System Administration interface:

- Administration Window Header, page 1-7
- Content Area, page 1-7
- Typing and Selecting Information in Fields, page 1-7
- Validating Information in Fields, page 1-7
- Validating Information in Windows, page 1-7

Administration Window Header

The header at the top of all Cisco TelePresence System Administration windows contains the name of the person currently logged in and provides links for the following functions:

- **Logout**—Click to log out of the system.
- **Help**—Click to display online help for using the Cisco TelePresence System Administration.
- **About**—Click to display software version and licensing information.

Content Area

The frame on the right is the content area, and the gray bar above the content area shows the navigational path so you can quickly identify where you are at any time.

Typing and Selecting Information in Fields

To modify information in fields, use the mouse to highlight and delete existing information. Type in new information. Some fields offer drop-down menus from which you choose settings.

Validating Information in Fields

Some Cisco TelePresence System Administration windows contain **Apply** and **Reset** buttons, which are initially disabled. Once you change or add settings in these windows, both buttons become enabled.

- Use the **Apply** button to apply new or modified information. When you click **Apply**, validation is performed for all fields in that window, and a message is displayed if there is invalid data in the fields.
- Use the **Reset** button to discard changes and restore the values shown when the window was first displayed.

Other Cisco TelePresence System Administration windows have fields containing information such as IP addresses, domain names, media port numbers (view only), and so on, that are validated when you exit the field. When information in a field is found to be invalid, a message describing the error is displayed.

Note View only fields such as stop and start media port numbers can be configured by going to **Devices > Device Settings > SIP Profile** in the Cisco Unified CM Administration interface. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* on Cisco.com for more information.

Validating Information in Windows

When you go to the navigation pane and click a task, the Cisco TelePresence System Administration software checks data in the current window and takes an action, as follows:

- If all changes are saved, the content area displays the requested window.

- If there are unsaved changes in the current window and data is valid, a message reminds you that there are unsaved changes. An **OK** button saves the changes, and a **Cancel** button allows you to continue modifying data.
- If there are unsaved changes and the data is not valid, a message explains what to do and provides **OK** and **Cancel** buttons to assist you.

Note If you change settings and click **Apply** in the navigation pane, the request may take a few moments to take effect. Wait until the pending request is completed before clicking a new task.

Troubleshooting Tabs

Cisco TelePresence System Administration includes a diagnostics interface for the Cisco TelePresence System EX Series (CTX). To access all available troubleshooting tasks, go to **Troubleshooting > Hardware Setup** and select one of the following tabs:

- Device Test
- CTX Tests

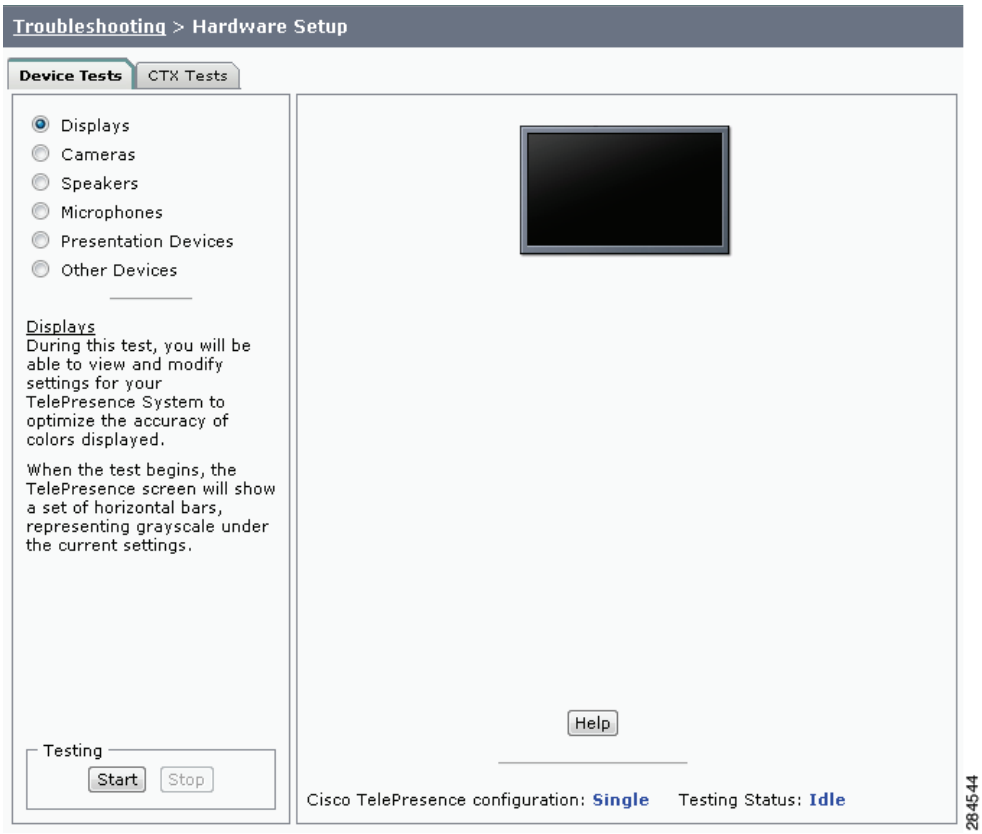
Device Test

The Device Tests tab provides the traditional Hardware Setup troubleshooting tasks for the following Cisco TelePresence System peripherals:

- Devices
- Cameras
- Speakers
- Microphones
- Presentation Devices
- Other Devices

Figure 1-4 shows the CTS device troubleshooting window.

Figure 1-4 CTS Device Troubleshooting Window



CTX Tests

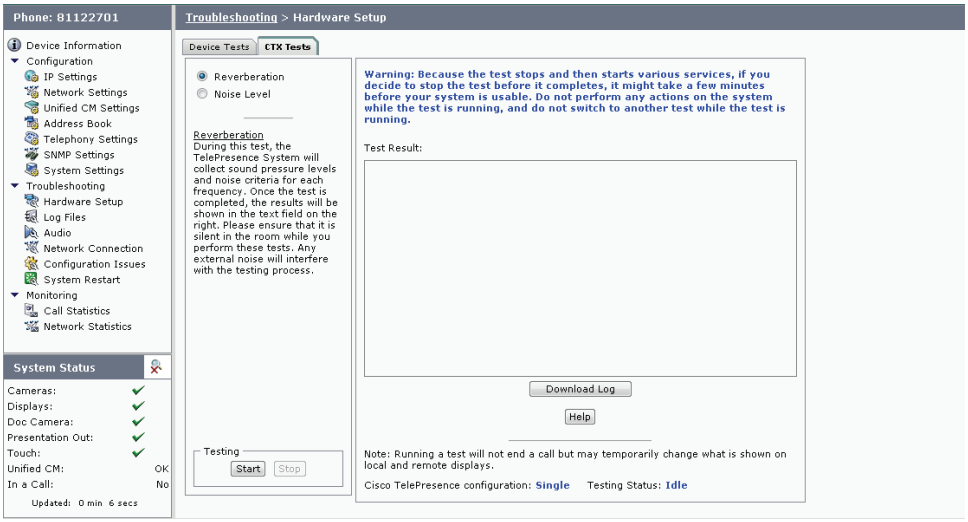
The CTX Tests tab provides acoustic tests to determine the acoustic suitability of a room for the installation of a Cisco TelePresence system. You can perform the following acoustic tests:

- Reverberation
- Noise Level

Note Because the test stops and then starts various services, if you decide to stop the test before it completes, it might take a few minutes before your system is usable. Do not perform any actions on the system while the test is running, and do not switch to another test while the test is running.

Figure 1-5 shows the CTX Tests window.

Figure 1-5 CTX Tests



Reverberation

The reverberation test measures how long it takes for sound waves in the room to decrease by 60 decibels.

When sound waves are generated in an enclosed environment, they continue to reflect from surface to surface until the energy is completely absorbed. This reflection of sound is called reverberation. Reverberation is measured as the rate of time in milliseconds (ms) for sound to decay by 60 decibels (RT60). Ideal conditions for human speech intelligibility are an RT60 value of 300 to 500 milliseconds for all frequencies between 125 Hz and 4 kHz. An extreme in either direction - too much reverberation or too little - can be detrimental to speech intelligibility, and since Cisco TelePresence is generally located in a meeting room in which the human voice is the main source of audio, an ideal sound-quality design preserves the human range of frequencies and isolates this range from interruptions.

For a more thorough discussion of room acoustics and reverberation, and the effect on telepresence conferencing, see the *Cisco TelePresence Room Design Guide*.

To perform a reverberation test:

Step 1 From left panel of the CTS Administrative UI, select **Troubleshooting > Hardware Setup**.

Step 2 Select the **CTX Tests** tab.

Step 3 Select the **Reverberation** radio button.

Step 4 Click **Start**.

The reverberation test will take several minutes to complete. Once complete, the CTS will restart. During the time of the test, and while the CTS is restarting, you will not be able to make telepresence calls.

Note It is important that the room be as silent as possible during the test.

Note The CTS will produce loud tones during while running the test. Cisco recommends exiting the room while the test is running.

After the test is complete, the CTS Administrative UI will display the results of the test, showing the RT60 in milliseconds (ms) at various frequencies. A sample of the test output is below:

```
Enter Reverberation Test Thu Dec 15 08:36:31 2011
M 125Hz  250Hz   500Hz   1000Hz  2000Hz  4000Hz
1 0.00   360.00  450.00  480.00  420.00  360.00
```

In the above example, a tone at 250 Hz had an RT60 of 360 ms, a tone played at 500 Hz had an RT60 of 450 ms, and so on. If the RT60 ranges for all of the measured frequencies fall between 300 ms and 500 ms, the reverberation in the room is ideal for a Cisco TelePresence system.

Noise Level

The noise level test measures the background noise present in the room. The noise level test measures background noise in decibels with A-weighting (dBA). The Cisco TelePresence system is designed to work in rooms with background noise levels of 45 dBA or lower. Background noise levels above 45 dBA begin to compete with the intelligibility of human speech, and these noises become distracting for participants. Background noise levels over 55 dBA can cause gating or sound suppression effects in the Cisco TelePresence audio.

For a more thorough discussion of room acoustics and noise levels, and the effect on telepresence conferencing, see the *Cisco TelePresence Room Design Guide*.

To perform a noise level test:

Step 1 From left panel of the CTS Administrative UI, select **Troubleshooting > Hardware Setup**.

Step 2 Select the CTX Tests tab.

Step 3 Select the Noise Level radio button.

Step 4 Click **Start**.

The noise level test will take several minutes to complete. Once complete, the CTS will restart. During the time of the test, and while the CTS is restarting, you will not be able to make telepresence calls.

Note It is important that the room be as silent as possible during the test.

Note The CTS will produce loud tones during while running the test. Cisco recommends exiting the room while the test is running.

After the test is complete, the CTS Administrative UI will display the results of the test, showing the average ambient noise level in decibels, as well as the noise level in decibels at a range of frequencies. A sample of the test output is below:

```
Enter Noise Level Test Thu Dec 15 08:46:50 2011
M  dBASPL       125Hz   250Hz   500Hz   1000Hz  2000Hz  4000Hz
1  42.06       46.51    41.47   40.73   32.78   26.52   27.63
```

In the above example, the average ambient noise was measured at 42.06 dBA (decibels), the ambient noise at 125 Hz was measured at 46.51 dBA, the noise level at 250 Hz was 41.47 dBA, and so on. An average measurement of 45 dBA or lower indicates that the noise levels in this room are acceptable for the installation of a Cisco TelePresence System.

Accessing Online Help

Online help describes the Cisco TelePresence System Administration graphical user interface (GUI). Use the following information to find information in the online help screens:

- Navigating Online Help, page 1-12
- Accessing this Administration Guide From Online Help, page 1-13

Navigating Online Help

To access online help:

Step 1 In the Cisco TelePresence Administration window, click the **Help** button or click **Help** in the toolbar in the upper right corner of the Cisco TelePresence System Administration screen. The Cisco TelePresence System Administration Online Help window appears.

Step 2 Click the **Contents** tab to navigate through online help topics.

Step 3 Click the **Index** tab to navigate through the list of online help terms and topics. You can type a keyword to locate specific information.

Step 4 Click the **Favorites** tab to manage frequently used subjects within the online help.

a. Click a subject in the **Contents** tab.

b. Select the **Favorites** tab to view the Current Topic that you selected in the Contents tab.

c. Click **Add** to save to Favorites.

d. Click **Remove** to delete from Favorites.

Step 5 Use **Hide**, **Back**, **Forward**, and **Print** to navigate through the online help windows.

Step 6 Click **Print** to print a copy of the online help page.

Accessing this Administration Guide From Online Help

Online help mirrors what you can see in the Cisco TelePresence System interface. When you need more information about a topic that you find in the online help, you can access the Cisco TelePresence System Administration Guide (this document) from the menu bar on the Cisco TelePresence System Administration screen.

To access the Cisco TelePresence System Administration Guide from Online Help:

Step 1 Choose **Help > View PDF**.

Step 2 Save or open the file when prompted.

Note For the most up-to-date information, including detailed testing and troubleshooting procedures, see the *Cisco TelePresence System Administration Guide* for your release on Cisco.com.

Where to Go Next

Proceed to Chapter 3, "Device Information" to access the Cisco TelePresence System Administration interface.

Understanding the Fields In the Cisco TelePresence System Administration Interface

Revised: April 2013, OL-28614-01

Contents

This chapter contains the following sections:

Fields in the Configuration Area

This section contains information about the fields that are in the Configuration area and contains the following topics:

IP Settings

The IP Settings window displays the CTS MAC address and hostname and you can view and manage the following:

- DHCP—Choose **Yes** if your network uses the Dynamic Host Configuration Protocol (DHCP) to dynamically assign a network address for your system. Choose **No** to assign a static address for your system if your network does not use DHCP.
- Domain name
- IP Address
- Default gateway
- DNS servers.

For more information about this field, see the "IP Settings" section on page 4-10.

Network Settings

You can view or configure the following settings in the Network Settings window:

- Operational VLAN ID
- Administrative VLAN ID
- Syslog Address

For more information about this field, see the "Network Settings" section on page 4-12.

Unified CM Settings

This field allows you to view and configure TFTP server locations and view a list of available settings for this Cisco TelePresence system. For more information about this field, see the "Cisco Unified Communications Manager Settings" section on page 4-13.

Address Book

The Address Book window displays read-only entries that have been set in Unified CM. You can create favorites for up to 40 meeting rooms.

To view the phone list of Cisco TelePresence system-enabled meeting rooms, follow these steps:

Step 1 Choose **Configuration > Address Book**.

Step 2 Use Unified CM to make changes to the Address Book. To add entries to the address book, refer to the "Managing the Speed-Dial Directory (Favorites)" section of the See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Telephony Settings

The Telephony Settings window displays read-only information about the telephony settings for the Cisco TelePresence System that were set in Unified CM. For more information about this field, see the "Telephony Settings" section on page 4-16.

SNMP Settings

Use this field to view a report of the SNMP configuration. For more information about this field, see the "SNMP Settings" section on page 4-18.

System Settings

This field allows you to view Unified CM configuration settings for your system. For more information about this field, see the "System Settings" section on page 4-20.

Security Settings

Use this field to view or download the MIC or LSC certificates that are used for your system. For more information about this field, see the "Security Settings" section on page 4-22.

Fields in the Troubleshooting Area

This section describes the fields that are available in the Troubleshooting area and contains the following topics:

Hardware Setup

Cisco TelePresence System Administration includes a diagnostics interface for the Cisco TelePresence System EX Series (CTX).

To access all available troubleshooting tasks, go to **Troubleshooting > Hardware Setup**.

If your GUI has tabs visible in this window, select one of the following tabs:

- Device Test: You can use the following Cisco TelePresence system troubleshooting features:
- CTX Tests (Not Available on All Systems): Test reverberation and noise levels for some systems (not available for all systems).

Note Not every system has the CTX test available; in this case, the tab is not visible.

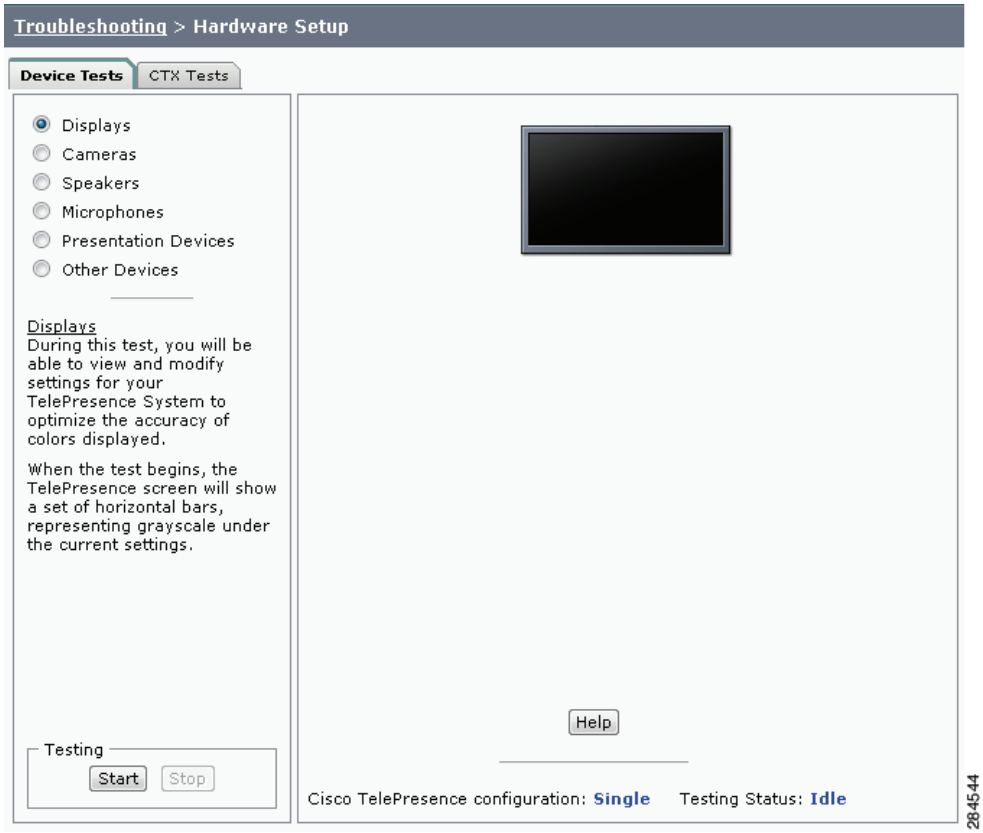
Device Test

The Device Tests tab provides the traditional Hardware Setup troubleshooting tasks for the following Cisco TelePresence System peripherals:

- Devices
- Cameras
- Speakers
- Microphones
- Presentation Devices
- Other Devices

Figure 2-1 shows the CTS device troubleshooting window.

Figure 2-1 CTS Device Troubleshooting Window



CTX Tests (Not Available on All Systems)

The CTX Tests tab provides the following troubleshooting tasks for the CTX:

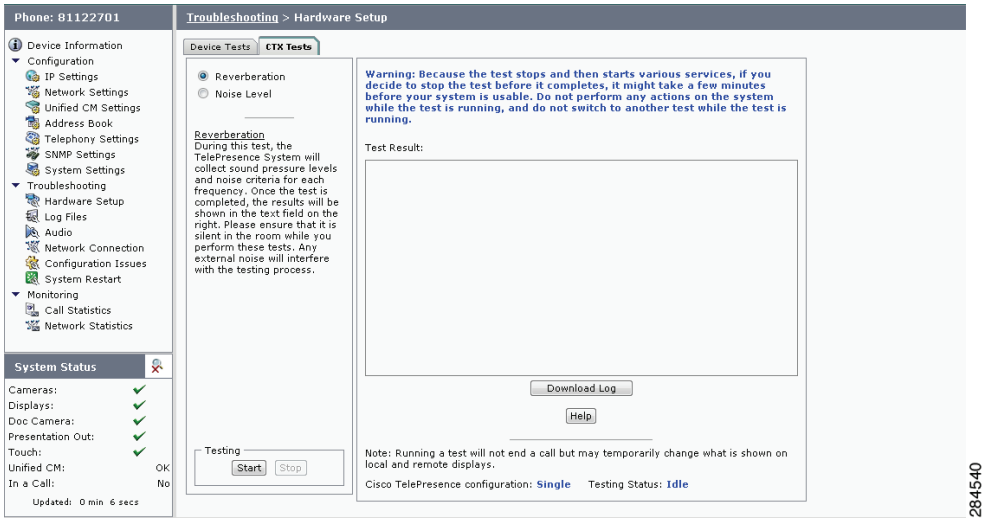
- Reverberation
- Noise Level

Note Running a test will not end a call but may temporarily change what is shown on local and remote displays.

Because the test stops and then starts various services, if you decide to stop the test before it completes, it might take a few minutes before your system is usable. Do not perform any actions on the system while the test is running, and do not switch to another test while the test is running.

Figure 2-2 shows the CTX Tests window.

Figure 2-2 CTX Tests



Reverberation

During this test, the Cisco TelePresence System collects sound pressure levels and noise criteria for each frequency. Once the test is completed, the results are shown in the Test Results.

Tip Ensure that the room is silent while you perform these tests. Any external noise will interfere with the testing process.

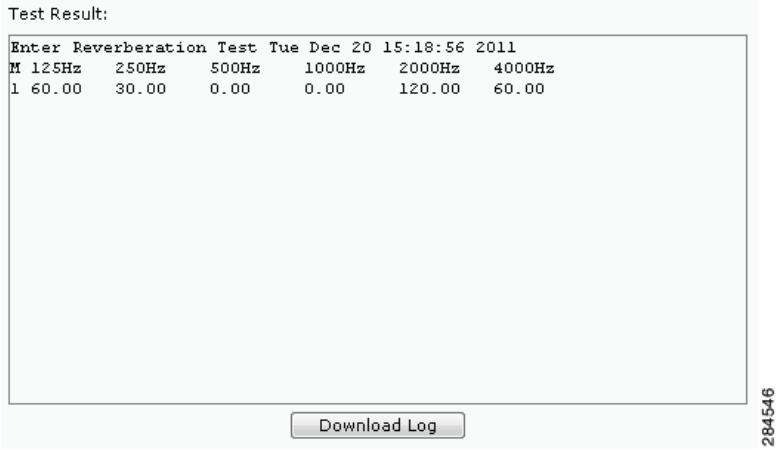
Step 1 Select the Reverberation radio button and then click **Start**.

The system issues the following information:

"Test Running: Test is running. Please wait until the test completes; if you stop the test, no results will be recorded."

The test takes a few minutes to complete. When complete, system reverberation information is displayed in the Test Results window, as shown in Figure 2-3.

Figure 2-3 Reverberation Test Results



Step 2 If desired, click **Download Log**.

The system asks whether you want to open or save the .txt file. This completes the reverberation test.

Noise Level

During this test, the Cisco TelePresence System plays audio chirps and collects the average sound decays for each frequency. Once the test is completed, the results are shown in the text field.

Tip Ensure that the room is silent while you perform these tests. Any external noise will interfere with the testing process.

Step 1 Select the Noise Level radio button and then click **Start**.

The system asks you if you want to continue with the test.

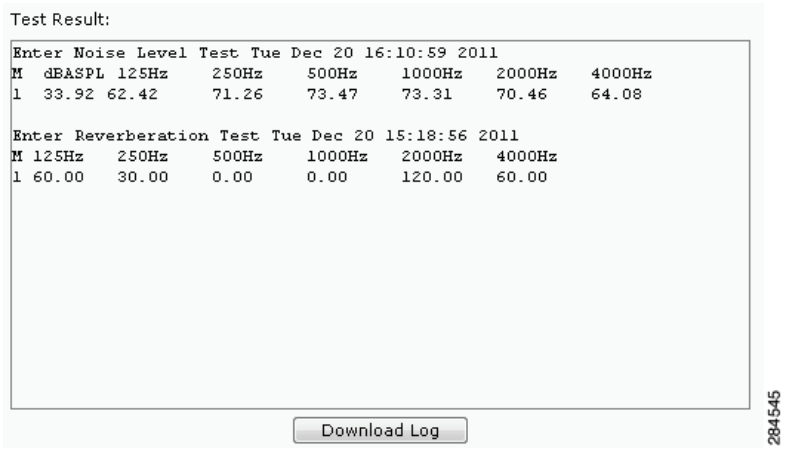
Step 2 Click **OK** in the dialog to begin the test.

The system issues the following information:

"Test Running: Test is running. Please wait until the test completes; if you stop the test, no results will be recorded."

The test takes a few minutes to complete. When complete, system noise level information is displayed in the Test Results window, as shown in Figure 2-4. If you have already run a reverberation test, the noise level test will appear at the top of the window.

Figure 2-4 Noise Level Test Results



Step 3 If desired, click **Download Log**.

The system asks whether you want to open or save the .txt file. This completes the noise level test.

Diagnostics

The Diagnostics window contains choices to diagnose issues with either your display or camera and contains the following pull-downs:

- **Display**: Contains the following tests:
  - **Display OSD state**: Shows the state of the on-screen display (OSD) service. The OSD service controls the appearance of on-screen icons during meetings.
  - **Display On/Off**: Shows the power status of the display (on or off).
  - **Display Edid**: Provides the Extended Display Identification Data (EDID) for the display.
  - **Display Error Status**: If the system detected an error with the display, this field shows the status of the error and also provides status of the power supply for the display.
  - **Display Diagnostics**: Shows the diagnostic information for all system displays.
  - **Display Information**: Shows the following information about the display. This information is useful in troubleshooting problems:

```
Center Display
Main Tx:
Port Address: 0x72.
VENDOR_ID=0x01
DEV_ID=0x9134
DEV_REV=0x1
Aux Tx:
Port Address: 0x76.
VENDOR_ID=0x01
DEV_ID=0x9134
DEV_REV=0x1
Main Rx:
Port Address: 0x60.
VENDOR_ID=0x01
DEV_ID=0x9135
DEV_REV=0x4
Aux Rx:
Port Address: 0x62.
```

```
VENDOR_ID=0x01
DEV_ID=0x9135
DEV_REV=0x4
```

- **Camera**: you can troubleshoot the camera using any of the following choices:
  - **Camera Cable Connectivity**: This checks the physical cable connections of the power and signal cables for the camera.
  - **Camera Reset**: Resets the cameras.

Note Resetting the cameras does not remove any changes you made to the auto brightness, luminance, auto color brightness, and flicker reduction settings to the cameras.

  - **Camera Settings:** Provides you with a list of the current camera settings. You cannot change these settings. The following are output examples:

```
Center Camera
flickerCompensation=false
autoBrightness=false
autoColorBalance=false
focusDistance=4
targetLuminance=35
```

  - Camera Settings File: Shows the setting as stored in the camera settings file.

Note The luminance values might differ between the settings shown here and the setting shown from the Camera Settings test; this is normal.

```
Center Camera
set gain 2.36205
set gain_red 1.21544
set gain_blue 1.80757
set gain_green 1
set roi_A_start_x 0
set roi_A_start_y 0
set roi_A_width 1919
set roi_A_height 1079
#autoBrightness=false
set autogain off
set autointegration off
#flickerCompensation=false
set integration 100
#targetLuminance=35
set target_luminance 60
#autoColorBalance=false
set whitebalance off
```

- **LCU**: Check the status of the Light Control Unit (LCU), if present on your system.

Log Files

The Log Files window contains three tabs:

- **Sysop logs**: Contains the System Operation (sysop) logs. For detailed explanations of teach of the sysop logs, refer to the *Cisco TelePresence System Message Guide*.

- **Log files**: These are files that are generally used by Cisco Technical support when troubleshooting system issues. Use this choice if directed by your Cisco technical support representative.
- **SIP messages**: These messages are related to SIP negotiation when setting up and ending a call.

Sysop Logs

View system operation (sysop) messages, including call information, call statistics, and call errors for the Cisco TelePresence system from this selection. There can be up to 20 individual files saved on the CTS, and each file can contain up to 100,000 characters.

To download the sysop log files, click the Download Sysop Files button at the bottom of the page. CTS Administration software then prompts you to do one of the following:

- Open to view the sysop log files—The last 100,000 bytes of the log are shown. When you download Sysop files, all available Sysop files will be downloaded.
- Save the sysop log files.

Log Files

Use this selection to retrieve log files from the Cisco TelePresence system. Log files can be retrieved from the CTS or from the CTS Cisco Unified IP phone. You can also retrieve log files from the Cisco TelePresence Touch 12 by tapping **More > Status > Report Problem**.

To manage log files:

Step 1 Choose Troubleshooting > Log Files.

Step 2 Select the Log Files tab. The following fields are displayed:

- Log Status—Shows the status of the log capture, including the percentage completed.
- Time Generated—Shows the time of the most recent log file capture.
- Problem—Problem Type can be one of the following:
  - Audio (Speakers, Microphones)
  - Video (Displays, Cameras)
  - Projector, LCD, document camera
  - Phone
  - Recording
  - Other/Unknown

Step 3 Choose from one of the following file download options:

- Download existing log files
- Capture and download new log files—The system will capture but not download the log files if your have pop-up blockers enabled for your system; in this case, either disable pop-up blockers for your browser, or select **Capture and download new log files** and then selecting **download existing log files.**
- None —Default. No log files will be captured unless a download option is selected.

Step 4 From the Select Problem Type drop-down menu, choose the type of problem you are experiencing:

- Audio (speakers, microphones)

- Video (displays, cameras)
- Projector, LCD, document camera
- Phone
- Recording
- Other/Unknown

Step 5 Click the **Get Log Files** button. The following message appears:

"A WinZip download will start within several minutes. Please wait..."

Or

"Collecting Cisco TelePresence system log files. This may take several minutes. Please wait..."

Tip The "Get Log Files" button is deactivated while the system captures the requested log files and is reactivated when complete.

The File Download window appears prompting you to open or save the file. Click Save to send the gzip file to Cisco technicians to help solve the problem.

SIP Messages

Session Initiation Protocol (SIP) request and response methods are used to establish communications between components in the network and ultimately to establish a call or session between two or more endpoints. Table 4-7 and Table 4-8 describe the SIP requests and message types.

To manage SIP messages:

Step 1 Navigate to **Troubleshooting > Log Files** and click the Select the **SIP Messages** tab.

The SIP Messages window appears.

Step 2 View a specific type of message in the SIP log file by performing one of the following actions:

- Enter the filter where the SIP Message Type is by typing the name in the field provided. The Filter button is activated.
- Select the message type from the drop-down menu and click the Filter button to view the SIP messages of the type you specified.

Step 3 Choose the number of messages to view at one time from the Rows Per Page drop-down menu. Use the First, Previous, Next, and Last buttons to navigate through the message list with the Navigating Long Lists option. You can also Generate Detailed Message Reports.

Step 4 To see additional details associated with a SIP message, perform one of the following actions:

- Double-click on a SIP message from the list to open the SIP Message Details dialog box. The SIP Message Details dialog box opens containing the message details and Related SIP Messages.
- Highlight the SIP message and click the Details button. The SIP Message Details dialog box opens containing the message details and Related SIP Messages.

Related SIP Messages

The bottom portion of the SIP Message Details window lists SIP messages that are related to the SIP message that was selected at the top of the window.

To view related SIP message details, Double-click a message in the Related SIP Messages window to see details for that message. SIP Requests and Methods and SIP Response Categories are explained in the following table.

Click **Close** to dismiss this window.

Use the information in the following sections to understand and navigate SIP requests and responses:

SIP Requests and Methods

SIP Response Categories

SIP Requests and Methods

Table 2-1 summarizes the SIP requests and methods supported by the Cisco TelePresence System Administration software. The first column lists the RFC that describes the SIP request messages or method.

Table 2-1 Supported SIP Requests and Methods

RFC	Request/Method	Description
3261	ACK	Confirms that the client has received a final response to an INVITE request.
3261	BYE	Terminates a call. Can be sent by either the caller or the called party.
3261	CANCEL	Cancels any pending searches but does not terminate any call currently in progress.
2976	INFO	Allows session-related control information generated during a session to be carried along the SIP signaling path.
3261	INVITE	Indicates that a user or service is being invited to participate in a call session.
3265	NOTIFY	Immediately upon successful accepting or refreshing of a subscription, a NOTIFY message is sent to communicate the current resource state to the subscriber. This NOTIFY message is sent in the same dialog as that created by the SUBSCRIBE message.
3261	OPTIONS	Queries the capabilities of servers.
3262	PRACK	Provides reliability for 1xx type messages. See Table 2-2.
3515	REFER	Provides a mechanism allowing the party sending the REFER message to be notified of the outcome of the referenced request.
3261	REGISTER	Registers the address listed in the To header field with a SIP server.
3265	SUBSCRIBE	Requests current state and state updates from a remote node.
3311	UPDATE	Allows a client to update parameters of a session, but has no impact on the state of a dialog. This request can be sent before the initial INVITE has been completed, thereby making it useful for updating session parameters within early dialogs.

SIP Response Categories

SIP replies to the requests in Table 2-1 using the response categories described in Table 2-2.

Table 2-2 SIP Response Categories

Response Category	Response Type
1xx	Informational messages
2xx	Successful responses
3xx	Redirection responses
4xx	Request failure responses
5xx	Server failure responses
6xx	General failure responses

Navigating Long Lists

The log file can hold up to 2 MB worth of SIP messages. To navigate long lists:

Step 1 Choose the number of rows that you wish to see on one page from the Rows Per Page drop-down menu.

Step 2 Double click to select and open single message details. The SIP Message Details window appears.

Step 3 If there are multiple pages listing log files, click the **First**, **Previous**, **Next**, or **Last** button to navigate to the desired page.

Step 4 Click the radio button to the left of the table entry, and then click **Clear** to delete a single error message.

Step 5 Click **Clear All** to delete all error messages displayed.

Related Information

For more information, refer to the following documentation:

- The Session Initiation Protocol (SIP) home page on Cisco.com.
- The *Cisco TelePresence System Message Guide*

Touch Screenshot

To take a screenshot of the current image on your CTS Touch device, navigate to **Troubleshooting > Touch Screenshot** and click **Capture New Touch Screenshot**. A screenshot of what is currently displaying on the Touch device for your system appears in the CTS administration GUI.

You can view this image or save it.

Audio

To take an audio recording of your CTS conference, navigate to **Troubleshooting > Audio** and click **Start Recording Audio**. The audio records for a maximum of two minutes or until you click **Stop Audio Recording**.

The recording is saved as a .tar file that contains an .mp4 file that can retrieve, unzip, open, and play.

This option is useful to troubleshoot audio issues with your system.

Network Connection

To change the Ethernet parameters of your network connection, navigate to **Troubleshooting > Network Connection**. This window contains the following choices:

- **Auto Negotiation**: Enables or disables auto negotiation by clicking the **On** of **Off** radio button. Turning off auto negotiation might require you to specify the speed of your connection manually.
- **Duplex**: Changes the duplex method from full-duplex to half-duplex, or vice versa, by clicking the **Full** or **Half** radio button. Only active is Audio Negotiation is set to Off.
- **Speed**: Changes the speed of your Ethernet connection.

Configuration Issues

Use this window to check the software images that are stored and running on your codec(s). You can also restart the system from the factory software image from this window.:

This window contains the following information:

- **Unit** (only for systems with more than one codec): Shows the codec position (left, center, or right) as viewed from the table side of the system.
- **Hardware version**: shows the hardware version of the codec(s).
- **Slot 1 image**: Shows the image that is stored on slot 1 of the system.

  The active image for the system is shown in bold, with an asterisk next to it.
- **Slot 2 image**: Shows the image that is stored on slot 2 of the codec(s).
- **Factory image**: Shows the image that was preloaded on the codec(s) from the factory.

To reload the codec from the factory image and restart the system, click the **Revert to Factory Configuration and use Cisco TelePresence image specified in Cisco Unified CallManager...and Restart TelePresence System...** button.

After the image reboots, it loads the system from the image that is in slot 0.

While the system is booting, an IP address display on the main display screen (the center display screen for three-screen systems). Make a note of the IP address to log into your system. After you log in to your system, you need to re-register to your Unified CM by navigating to **Configuration > Unified CM Settings**, specifying the IP address of the Unified CM server, and clicking **Apply**.

System Restart

This If you reboot your system, the codec reboots from the active image.

To restart your system, click the **Restart Cisco TelePresence System...** button. Clicking this button reloads the codec from the image that is specified as the default image in Unified CM and restart the system. If there is no image specified in Unified CM, the system boots from the active image.

To see the active image, navigate to **Troubleshooting > Configuration Issues**. The active image displays in bold with an asterisk next to it.

Fields in the Monitoring Area

This sections describes the fields that are available in the Monitoring area and includes the following topics:

Call Statistics

Use the Call Statistics window to view audio and video statistics collected by the codecs. The reports include descriptions to help you understand the type of information that is being collected.

To view call statistics:

Step 1 Choose **Monitoring > Call Statistics**.

You can view the following Cisco TelePresence system statistics:

- **Real Time Call Statistics**—Lists details of an in-progress call, including the following:
  - Connection status
  - Registered to Unified CM
  - Local meeting number
- **Audio/Video Call**—Lists details about the audio and video of an in-progress call, including the following:
  - Call Start Time
  - Call Duration
  - Call Type
  - Remote meeting number
  - Call State
  - Actual Bit Rate
  - Negotiated Bit Rate
- **Historical Call Statistics (not including current call, if any)**—Lists historical information about calls including the following:
  - Call Statistics Clear Time
  - Last Call Start Time
  - Last Call Duration
  - Number of Calls Since System Setup
  - Time in Calls Since System Setup (seconds)
  - Number of Calls Since Last Reboot
  - Time in Calls Since Last Reboot (seconds)
  - Registered to Cisco Unified Communications Manager

– Configured Bit Rate

Step 2 For more specific audio and video statistics, click the check-box next to the following selections.:

- Audio/Video Call: Audio Stream Statistics
- Audio/Video Call: Video Stream Statistics
- Audio-Only Call: Stream Statistics

Audio/Video Call: Audio Stream Statistics

a. Click once to select. Additional statistics fields appear.

b. Click once to de-select. Additional fields are hidden.

See Figure 2-5.

Audio/Video Call: Video Stream Statistics

a. Click once to select. Additional statistics fields appear.

b. Click once to de-select. Additional fields are hidden.

Audio-Only Call: Stream Statistics

a. Click once to select. Additional statistics fields appear.

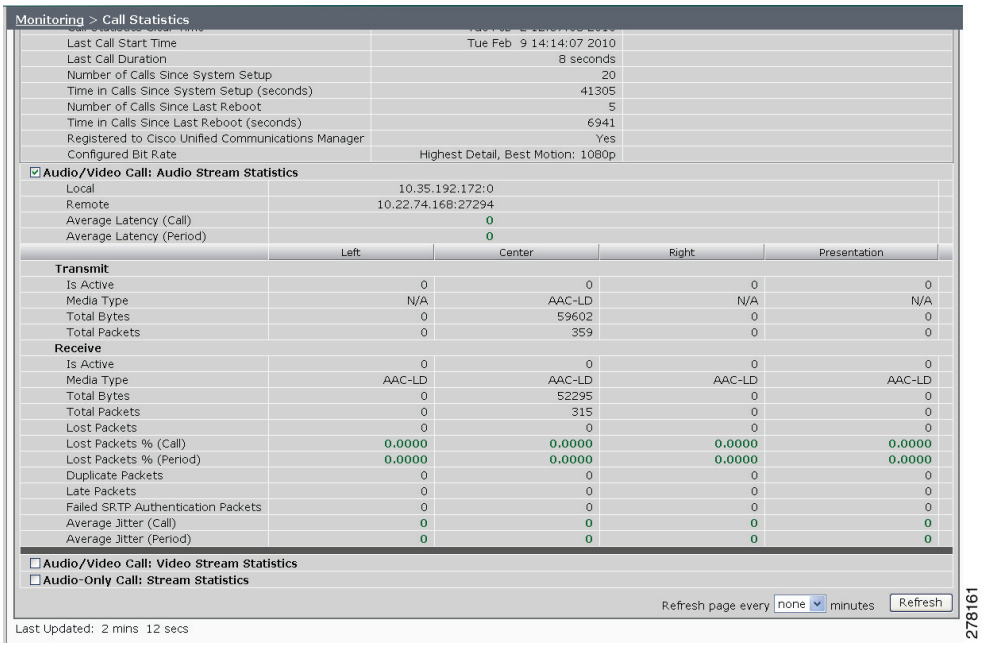
b. Click once to de-select. Additional fields are hidden.

Statistics are listed in columns labeled as if you were looking at the front of the system sitting at the conference table. For example, on a CTS 3000 or CTS 3200, the labels indicate statistics from the left, center, and right codecs (and presentation codec, if installed), and from auxiliary devices (when connected).

When you select one of the choices above, additional statistics fields appear with the following status information listed, as shown in Figure 2-5:

- Local
- Remote
- Average Latency (Call)
- Average Latency (Period)

Figure 2-5 **Audio/Video Call: Audio Stream Statistics**



Additional statistics are listed for the following, as shown in Figure 2-6:

- Transmit
- Receive

Transmit

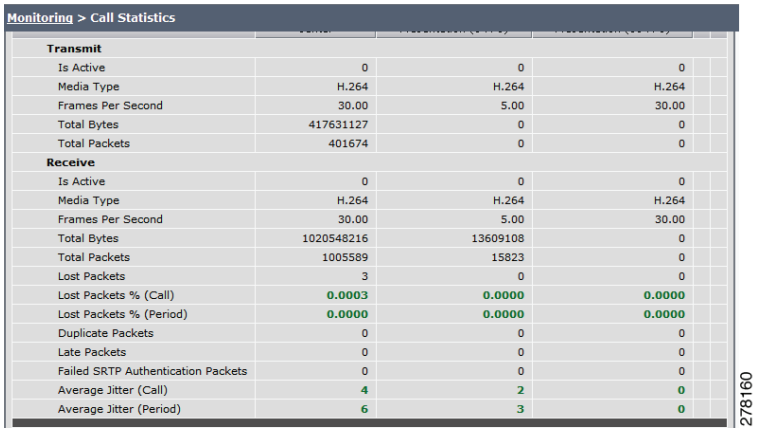
- Is Active
- Media Type
- Total Bytes
- Total Packets

Receive

- Is Active
- Media Type
- Total Bytes
- Total Packets
- Lost Packets
- Lost Packets % (Call)
- Lost Packets % (Period)
- Duplicate Packets
- Late Packets
- Failed SRTP Authentication Packets
- Average Jitter (Call) (see jitter call)
- Average Jitter (Period) (see jitter period)

Note For more information about jitter and packet loss, see the Understanding Jitter and Packet Loss Reporting section of the *Cisco TelePresence System Message Guide* on Cisco.com.

Figure 2-6 Call Statistics - Transmit and Receive



Monitoring > Call Statistics

Transmit			
Is Active	0	0	0
Media Type	H.264	H.264	H.264
Frames Per Second	30.00	5.00	30.00
Total Bytes	417631127	0	0
Total Packets	401674	0	0
Receive			
Is Active	0	0	0
Media Type	H.264	H.264	H.264
Frames Per Second	30.00	5.00	30.00
Total Bytes	1020548216	13609108	0
Total Packets	1005589	15823	0
Lost Packets	3	0	0
Lost Packets % (Call)	0.0003	0.0000	0.0000
Lost Packets % (Period)	0.0000	0.0000	0.0000
Duplicate Packets	0	0	0
Late Packets	0	0	0
Failed SRTP Authentication Packets	0	0	0
Average Jitter (Call)	4	2	0
Average Jitter (Period)	6	3	0

278160

Step 3 Set an interval for updating these reports by choosing the time from the Refresh drop-down menu. Choices, in minutes, include the following:

- None (default)
- 1
- 2
- 5
- 10
- 13
- 60

Step 4 Click **Refresh** to update the statistics immediately.

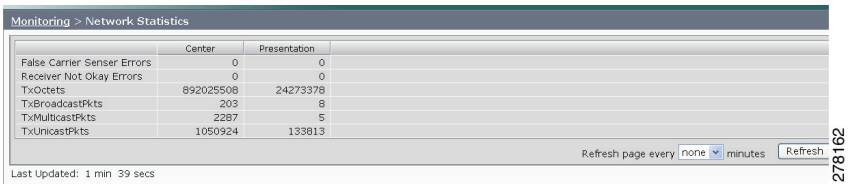
Network Statistics

Use Network Statistics to view packet transmission statistics collected from the network. Statistics are listed in columns labeled as if you were looking at the back of the system. For example, on a CTS 3000 or CTS 3200, the labels would indicate statistics from the left, center, and right codecs.

To monitor network statistics:

Step 1 Choose **Monitoring** > **Network Statistics**. Statistics for your system appear, as shown in Figure 2-7.

Figure 2-7 Network Statistics Window



Step 2 Look for error counters that have been incremented since the last time you viewed these statistics. Statistic types include the following:

- False Carrier Sensor Errors
- Receiver Not Okay Errors
- Number of TxOctets
- Number of TxBroadcastPkts
- Number of TxMulticastPkts
- Number of TxUnicastPkts

Step 3 Set an interval for updating these reports by choosing the time from the Refresh drop-down menu. Choices, in minutes, include the following:

- None (default)
- 1
- 2
- 5
- 10
- 13
- 60

Step 4 Click **Refresh** to update the statistics immediately.

Services Statuses

To check and, in some cases, restart network services, navigate to **Monitoring > Services Statuses**. You can restart the following services; to do so, click the **Restart** button next to the service to restart it:

- Dynamic Host Control Protocol (DHCP) server
- Simple Network Management Protocol (SNMP) server
- Calling Services
- The telephone server

Where to Go Next

Proceed to Chapter 3, "Device Information" to access the Cisco TelePresence System Administration interface.

Device Information

Created: April 2013, OL-28614-01

Contents

This chapter contains the following sections:

Accessing the Device Information Window

The Device Information window is the first thing you see when you log on to the Cisco TelePresence System Administration interface. It is from this window that you can access configuration, troubleshooting, and monitoring tasks for the Cisco TelePresence System (CTS) as well as view information about the devices installed on your system.

Before You Begin

To access the Cisco TelePresence System Administration interface for the first time, complete the steps in Logging into the Cisco Unified CM Administrator section of *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

To view information about the Cisco TelePresence devices on your system:

Step 1 Log in to the Cisco TelePresence System Administration interface by completing the following steps:

a. Open an Internet browser window and type in the IP address of the system in the URL field and click **Enter**. The Cisco TelePresence Administration Login Screen appears, as shown in Figure 3-1.

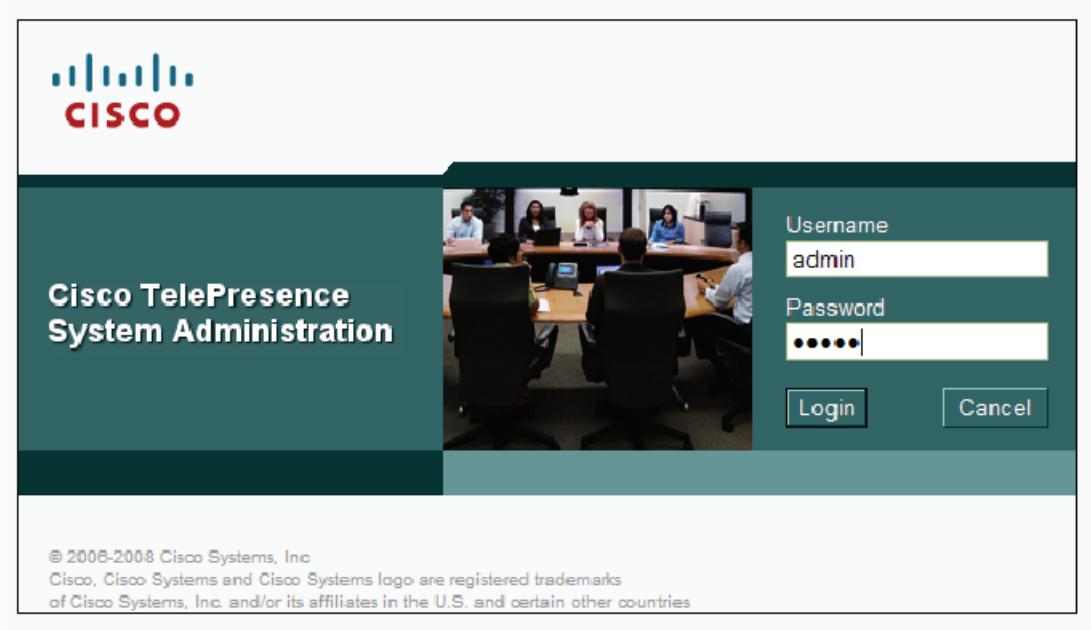
Note If you need to obtain the IP address, do the following:

1. On the IP phone, locate “Manual” at the bottom of the screen and press the **Manual** soft key.

   Or

2. Locate “Info” at the bottom of the screen and press the **Info** soft key.
3. Scroll down to the IP Address listing and copy the address.

Figure 3-1 Cisco TelePresence System Administration Login Screen



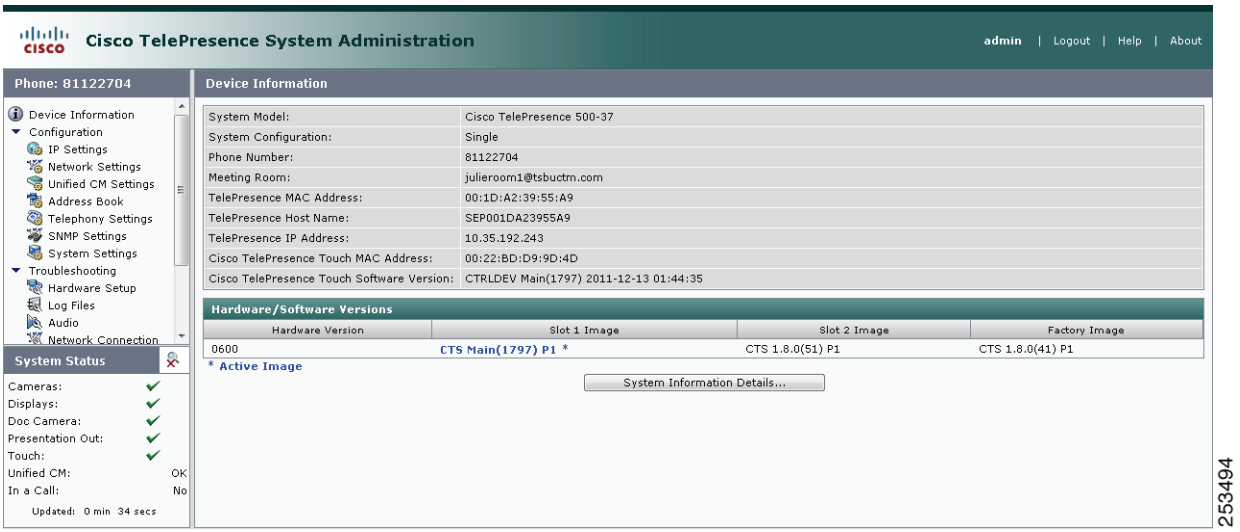
b. In the Admin field, type **admin**.
c. In the Password field, type **cisco**.

Note You can change the default password in Unified CM. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

d. Click **Login**.

The Device Information window appears, as shown in Figure 3-2.

Figure 3-2 Device Information Screen



Step 2 View the information in the following sections within the Device Information window:

- Device Information Fields
- Hardware/Software Versions
- System Information and Status Tabs

Device Information Fields

The Device Information area contains details about the settings that were configured in the CTS and the Unified CM. The information in Table 3-1 describes setting descriptions in the Device Information fields.

Note The Cisco TelePresence System device type must be specifically selected before you can upgrade to CTS Software Release 1.9.0 and later releases.

Table 3-1 Device Information Fields

Field or Button	Setting or Description
System Model	Your Cisco TelePresence System model.
System Configuration	Indicates the number of high-definition displays for this system.
Phone Number	Phone number of your system.

Table 3-1 Device Information Fields (continued)

Field or Button	Setting or Description
Meeting Room	Name of the meeting room in which this particular CTS is located as defined in Unified CM.
TelePresence MAC Address	MAC address of the primary CTS codec.
TelePresence Host Name	Host name of the primary CTS codec.
TelePresence IP Address	IP address of the primary CTS codec.
Cisco TelePresence Touch MAC Address	MAC address of the Cisco TelePresence Touch 12, if your system uses the touch device instead of the Cisco Unified IP phone for call control.
Cisco TelePresence Touch Software Version	Software version used by the Cisco TelePresence Touch 12, if your system uses the touch device instead of the Cisco Unified IP phone for call control.
IP Phone MAC Address	MAC Address of the IP phone as entered in Unified CM, if your system uses an IP phone for call control.
IP Phone Host Name	Host name of the IP phone as configured in Unified CM, if your system uses an IP phone for call control.
IP Phone IP Address	IP address of the IP phone as configured in Unified CM, if your system uses an IP phone for call control.
IP Phone Software Version	Version of the operating system software installed on this IP phone, f your system uses an IP phone for call control.

Hardware/Software Versions

Version information is collected from the hardware and software versions currently loaded in the system. In the Hardware/Software Versions area, data in bold **blue** text (with an asterisk "*") indicates which software image is currently running. Table 3-2 describes the hardware and software versions information fields.

Table 3-2 Hardware/Software Information Fields

Field or Button	Setting or Description
Unit	For Cisco TelePresence Systems with more than one codec. Indicates whether this is the left, center, right, or presentation codec.
Hardware Version	Version number of the codecs of the Cisco TelePresence System.
Slot 1 Image Slot 2 Image	The flash card is set up with three partitions for the software. Slot 1 and Slot 2 each hold a version of the codec software.
Factory Image	Software that is pre-loaded at the factory and the software that will be loaded after a factory reset.

System Information and Status Tabs

Information provided in the System Information Details window is used by Cisco technical support personnel to assist in troubleshooting your system.

To obtain a detailed report about the system:

Step 1 Log in to the Cisco TelePresence System Administration page. The Device Information window appears.

Step 2 Click the **System Information Details** bar. A new window opens.

Step 3 Click the following tabs in the new window:

- System Information Details
- Status Details

Step 4 Click **Close** to close the window.

System Information Details

Detailed system information is displayed per codec:

- One codec—For systems with one codec, all information displayed is for the system's single codec.
- Three codecs—For systems with three codecs, hardware and software information is displayed for left, center, and right codecs.
- Presentation codec—For systems that include a presentation codec, hardware and software information for the presentation codec is also displayed.

Table 3-3 describes the fields found in the System Information Details window.

Table 3-3 System Information Details Fields

Field or Button	Setting or Description
UDI_Hardware_Ver	Unique device identifier hardware version number.
UDI_Serial	Unique device identifier serial number.
UDI_PID	Unique device identifier product identification number.
System_Up_Time	Amount of time the system has been running since last reboot.
OS_Ver	Version number of the operating system.
OS_BuildTime	Time at which operating system was built.
UBOOT_Ver	Version number of the application that controls the boot process.
CF_Model	Compact flash model number.
Camera_PID	Camera product identification number.[1]
Camera_Hardware	Camera hardware number.[1]
Camera_Firmware_Ver	Camera firmware version number.[1]
Camera_Hardware_Ver	Camera hardware version number.[1]
Camera_BuildTime	Time at which the camera firmware version was built.[1]
Document_Camera_Serial	Document camera serial number.[2]
Document_Camera_Hardware_Ver	Document camera hardware version number.[2]
Document_Camera_Model	Document camera model number.[2]
Display_Serial	Serial number of the display.
Display_Hardware_Ver	Display hardware version number.
Display_Model	Display model number.
Display_BootCode_Ver	Version number of the boot loader for AppCode. BootCode also provides upgrade feature for AppCode.
Display_AppCode_Ver	Version number for AppCode. AppCode provides monitoring, managing control, and diagnostic functionality.
FPGA_ID	Field programmable gate array identification number.
FPGA_Rev	Field programmable gate array revision number.
FPGA_BuildTime	Time at which field programmable gate array was built.
MainRx_DevID	Main camera device identification number.
MainRx_Rev	Main camera revision number.
AuxRx_DevID	Auxiliary camera (document camera or VGA input device) device identification number.
AuxRx_Rev	Auxiliary camera (document camera or VGA input device) revision number.
MainTx_DevID	Main display (plasma) device identification number.
MainTx_Rev	Main display (plasma) revision number.
AuxTx_DevID	Auxiliary display device identification number.
AuxTx_Rev	Auxiliary display revision number.

Table 3-3 System Information Details Fields (continued)

Field or Button	Setting or Description
OSD_DEVICE1_BuildTime	On screen display (device 1) build time.
OSD_DEVICE5_BuildTime	On screen display (device 5) build time.
VCODEC_encoder_Card_Ver	Video CODEC encoder card version number.
VCODEC_decoder_Card_Ver	Video CODEC decoder card version number.
Audio_Hardware_Ver	Audio version hardware version number.
Audio_CPLD_Ver	Audio complex programmable logic device version number.
Audio_DSP_BuildID	Audio DSP software version.[3]
Audio_Base_BoardID	Type of audio base board. Choices are: • 0xAD • 0xAB
Audio_Base_Board_FAB_Ver	Hardware version of the audio (base) board
Audio_Base_Board_FW_Ver	Firmware version of the audio (base) board
Audio_Extension_UnitID	Type of audio extension board. The board type is either 0xAE or is disconnected.
Audio_Extension_Unit_FAB_Ver	Hardware version of the audio extension board.
Audio_Extension_Unit_FW_Ver	Firmware version on the audio extension board.
Audio_Clock_Source	Clock source syncing the audio and video streams.
Audio_PCB_S/N	CTS 500-37 and CTS 1300 only. Unique device identification (UDI) containing serial numbers unique to that printed circuit board (PCB).
Audio_PCB_P/N	CTS 500-37 and CTS 1300 only. Unique device UDI containing part numbers unique to that PCB.
Audio_PCB_Rev	CTS 500-37 and CTS 1300 only. Unique UDI containing hardware revision information unique to that PCB.
PoE_Reset_Available	Indicates whether Power over Ethernet (PoE) Reset feature is available.
Mfg_Installed_Cert	Security certificate for encryption defined by Cisco Root Certificate Authority.
Locally_Significant_Cert	Security certificate obtained through Certificate Authority Proxy Function (CAPF), which supersedes the manufacturing installed security certificate.
Max_Security_Setting	Configured security setting.
Aux Control Unit_Model	Auxiliary control unit model.
Aux Control Unit_Ver	Auxiliary control unit system firmware version.
Aux Control Unit_UDI_Vid	Auxiliary control unit unique device identifier version identification.
Aux Control Unit_UDI_Pid	Auxiliary control unit unique device identifier product identification number.
Aux Control Unit_UDI_Sn	Auxiliary control unit unique device identifier serial number

Table 3-3 System Information Details Fields (continued)

Field or Button	Setting or Description
Projector_Model	Projector model number, if projector is installed.
Presentation Display Model	Presentation display information.
Phone_midlet_status	Displays MIDlet status.
Phone_midlet_version	Displays MIDlet version

1. CTS 1300 displays information for Center, Left, and Right cameras.
2. The document camera is not available on the CTS 1300.
3. CTS devices are backward compatible up to two CTS Software Releases. Cisco recommends that you upgrade to the latest version software.

Status Details

Detailed status information is displayed per codec:

- One codec—For systems with one codec, all information displayed is for the system's single codec.
- Three or four codecs—For systems with three or four codecs, hardware and software information is displayed for those codecs.
- Presentation codec—For systems that include a presentation codec, hardware and software information for the presentation codec is also displayed.

Tip You can also view this window by returning to the Device Information window and clicking the magnifying glass icon in the upper right corner of the Status pane, which is in the lower left corner of the screen. See Figure 3-3 for an example of the magnifying glass icon and the Status pane.

Figure 3-3 CTS System Status

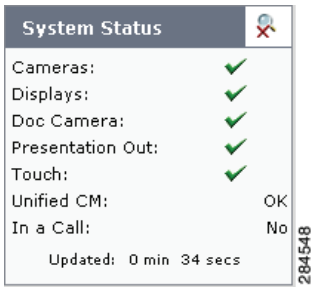


Table 3-4 contains descriptions of the Status Details fields. CTS displays a red X next to devices that are not operational or in error.

Table 3-4 Detailed Status Information Fields

Field	Setting or Description
Peripheral Status	**Cameras** • Video Cable Connection • Ethernet Connection **Note** CTS 1300 displays information for Center, Left, and Right cameras. **Displays** • Status **Microphones** • Status **Note** CTS 1300 displays information for the following microphones: – Positional (Center, Left, and Right) – Table (Center, Left, and Right) – Not used (ellipses) **Document Camera** • Video Cable Connection • Power Status • Unified CM Configuration • Ethernet Connection **Note** The document camera is not available on the CTS 1300. **Presentation Output Device** • Video Cable Connection • Power Status • Unified CM Configuration • Status • Lamp Age (hours) • Ambient Temperature • Lamp Temperature • LCD Temperature **IP Phone *or* Cisco TelePresence Touch** • Status

Table 3-4 Detailed Status Information Fields (continued)

Field	Setting or Description
System Status	• Unified CM • In a call • Audio/Video Expansion Box • Auxiliary Control Unit **Presentation Codec** • Unified CM Configuration • Status
Note	Further status information is located in the Time Since Last Update and Microphone Status sections at the bottom of the Status Details page.

Time Since Last Update

A running timer is located at the bottom of the Status Details page that displays elapsed time since last update.

Microphone Status

A roadmap of microphone status information icons is displayed at the bottom of the Status Details page.

- Ellipses—Not Expected / Not Connected.

- Green Check Mark—Connected.

- Question Mark—Not Expected / Not Connected.

- Red X—Not connected.

Note To determine individual microphone and speaker functionality, use the hardware troubleshooting interface for your system. See Where to Go Next to locate the troubleshooting support document for your Cisco TelePresence system.

Where to Go Next

Proceed to the following Cisco TelePresence system administration tasks from the Device Information window:

Configure

- Configuring the Cisco TelePresence System, page 4-1

Troubleshoot

Platform-specific troubleshooting:

Refer to the “First-Time Setup” chapter for your Cisco TelePresence System to run testing procedures for each of your system components:

- *Cisco TelePresence System 500-37 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence 1000 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 1100 Assembly, First-Time Setup, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 1300-65 Assembly, First-Time Setup, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3000 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3010 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3200 Assembly, Use & Care, and Field-Replaceable Unit Guide*
- *Cisco TelePresence System 3210 Assembly, Use & Care, and Field-Replaceable Unit Guide*

Monitor

- Monitoring the Cisco TelePresence System, page 5-1

Configuring the Cisco TelePresence System

Created: April 2013, OL-28614-01

Contents

This chapter contains the following sections:

Configuring Cisco Unified Communications Manager for Your Cisco TelePresence System

Before you can use your system, you need to configure your system in Cisco Unified Communications Manager (Unified CM).

You can configure your system and complete all steps in this chapter prior to configuring your device in Unified CM, but you will not be able to complete any of the following actions until you register your device:

- The Touch device cannot download its software from Unified CM and you receive an error in the logs.
- The Cisco TelePresence device cannot place or receive calls.
- The device appears as a Cisco TelePresence System 1000 in the Cisco TelePresence Administration GUI.

To configure your device in Unified CM, complete the following steps:

Step 1 Load the Cisco TelePresence Administration Software image on the Unified CM server.

For more information, refer to the following sections in the *Cisco Telepresence Touch 12 Installation Guide*:

- If you are upgrading from a software version that prior to 1.7.4, follow the steps in the "Upgrading the CTS Software for Systems That Are Running Cisco TelePresence Software Versions Prior to 1.7.4" section.
- If you are upgrading from a software version that is 1.7.4 or later, follow the steps in the "Upgrading the CTS Software for Systems That Are Running Cisco TelePresence Software Versions 1.7.4 and Above" section.

Step 2 Register your system as a device in Unified CM. For more information, refer to the "Configuring a Cisco TelePresence Device" section in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Step 3 Add the TFTP server for your Unified CM server to your system using the Cisco TelePresence Administration Software GUI. For more formation, refer to the "Cisco Unified Communications Manager Settings" of the *Cisco TelePresence System Administration Guide* for your software release.

For more information about configuring Unified CM with your Cisco TelePresence device, refer to the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

First Time Setup

To set up your Cisco TelePresence System (CTS) for the first time, you must first load the CTS Administration software and bootup the system.

This section contains the following information:

Loading CTS Administration Software

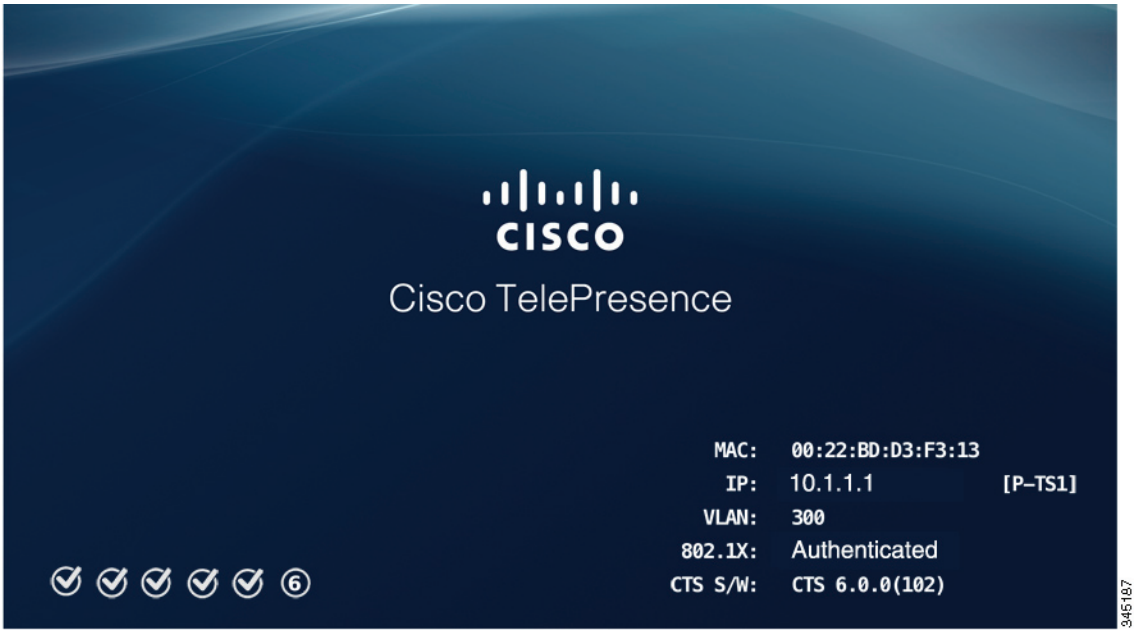
CTS Administration Software is factory-installed on each codec and loads during initial bootup. To boot up CTS Administration Software:

Step 1 Power on the PDU that is on the bottom of the CTS cabinet by turning the switch to the **On** position.

Step 2 Turn on the codecs that are associated with your CTS device. The displays associated with each codec become active. CTS displays green check marks on all displays to show bootup progress. Bootup is complete when the system displays six check marks. Figure 4-1 shows a screen with five of the six check marks checked.

Tip Ignore any messages that indicate a communication error with the camera; this message indicates that the system has not yet downloaded the correct software or firmware.

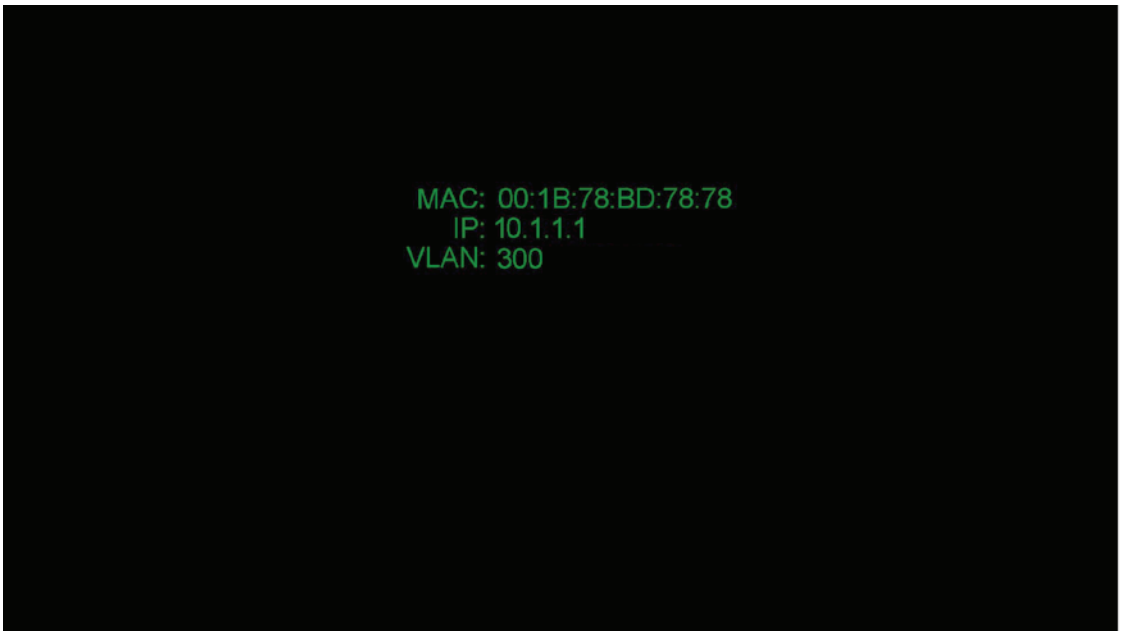
Figure 4-1 Bootup (Five of Six Check Marks Checked)



Note If the last check mark displayed is a red "X," there has been a compact flash error. If you receive this error, contact Cisco Technical Support.

Step 3 After bootup completes, make a note of the IP and MAC address that displays on the center of the screen, as shown in Figure 4-2. Use this information to log in to the Cisco TelePresence System Administration interface. This IP address displays until you log in to Cisco TelePresence System Administration or use Secure Shell (SSH) to log in to your CTS device.

Figure 4-2 System IP Address



Note If the IP address that displays is 192.168.100.2, the CTS device could not contact the DHCP server or your system does not use DHCP. Do one of the following:

1. If your network does not use DHCP, configure a static IP address using the information in the "Configuring a Static IP Address for Networks That Do Not Use DHCP" section on page 4-4.

Configuring a Static IP Address for Networks That Do Not Use DHCP

If your network does not use DHCP, complete one of the following procedures to configure a static IP address for your Cisco TelePresence system.

See the following sections to manage static IP addresses:

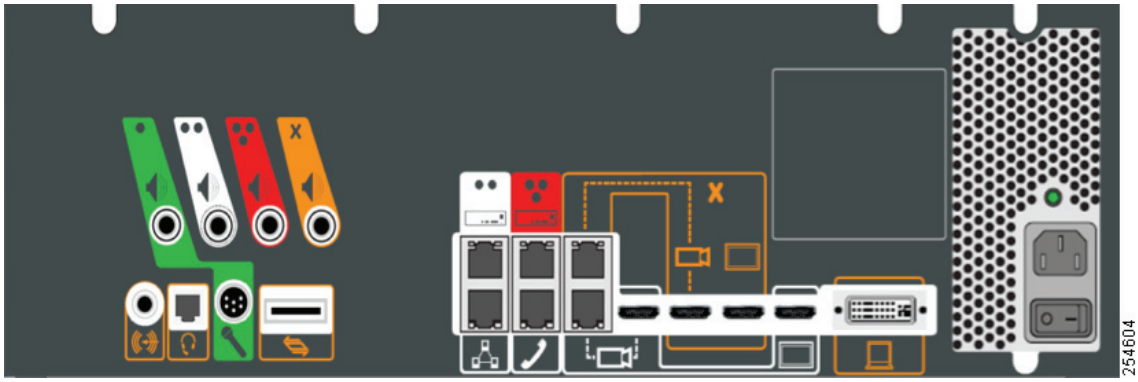
- Configuring a Static IP Address Using the Cisco TelePresence System GUI, page 4-5
- Configuring a Static IP Address Using Command-Line Interface Commands, page 4-6
- Command Example, page 4-6

Configuring a Static IP Address Using the Cisco TelePresence System GUI

To configure a static IP address using the Cisco TelePresence system GUI:

Step 1 Connect a DHCP-enabled PC to the secondary camera port of the primary codec. This connection is listed as the auxiliary network port in Figure 4-3.

Figure 4-3 Auxiliary Network Port Location



Step 2 Determine the IP address that the Cisco TelePresence system provided for your session.

Tip For Windows-based systems, you can see the IP address in the Support tab in the Local Area Connection Status window.

Step 3 Using Secure Shell SSH or another secure client program, start a CLI session with the Cisco TelePresence system using the IP address *xxx.xxx.xxx*.1,

Where:
xxx.xxx.xxx is the IP address that Cisco TelePresence provided for your session.

For example, if your determine that the Cisco Telepresence system provided an IP address of 10.1.0.2, enter the address 10.1.0.1.

By default, the username is **admin** and the password is **cisco**.

Step 4 Network services are started automatically. If needed, enter the following command to start network services:

utils service start Calling_Services

Step 5 Using a supported Internet browser, log in to the Cisco TelePresence system GUI with the IP address that you used in Step 3.

Step 6 Enter the username and password when prompted. By default, the user is **admin** and the password is **cisco**.

Step 7 Navigate to **Configuration > IP Settings**.

Step 8 Change the DHCP Enabled setting to **No**.

Step 9 Enter a static IP address, subnet mask, and IP gateway for your system into the fields. Optionally, enter DNS server(s) and the network domain name. Your system saves the changes and automatically restarts.

Step 10 Continue to the "Configuring Unified CM For Networks with a Static IP Address" section on page 4-7 to configure Unified CM for your system.

Configuring a Static IP Address Using Command-Line Interface Commands

To configure a static IP address using command-line commands:

Step 1 Connect a DHCP-enabled PC to the secondary camera port of the primary codec. This connection is listed as the auxiliary network port in Figure 4-3.

Step 2 Determine the IP address that the Cisco TelePresence system provided for your session.

Tip For Windows-based systems, you can see the IP address in the Support tab in the Local Area Connection Status window.

Step 3 Using Secure Shell SSH or another secure client program, start a CLI session with the TelePresence system using the IP address *xxx.xxx.xxx*.1,

Where:
xxx.xxx.xxx is the IP address that Cisco TelePresence provided for your session.

For example, if your determine that the Cisco Telepresence system provided an IP address of 10.1.0.2, enter the address 10.1.0.1.

By default, the username is **admin** and the password is **cisco**.

Step 4 Enter the following command to configure a static network IP address:

set network IP static *ip-address ip-subnet ip-gateway* [*dns-address*1][*dns-address2*][*domain-name*]

Where:

ip-address is the IP address of the system

ip-subnet is the IP subnet mask of the system

ip-gateway is the IP gateway of the system

dns-address1 is the IP address of DNS server 1 (Optional)

dns-address2 is the IP address of DNS server 2 (Optional)

domain-name is the domain name for the network (Optional)

Step 5 Continue to the "Configuring Unified CM For Networks with a Static IP Address" section on page 4-7 to configure Unified CM for your system.

Command Example

The following example gives the Cisco TelePresence system with an IP address of 10.0.0.2, a subnet of 255.255.255.0, a gateway of 10.0.0.1, a DNS server of 172.16.1.5, and a domain name of cisco.com:

```
admin:set network IP static 10.0.0.2 255.255.255.0 10.0.0.1 172.16.1.5 cisco.com
ip address successfully set
```

```
system restarting...
```

Configuring Unified CM For Networks with a Static IP Address

If your system uses a static IP address, manually specify the IP address of your Cisco Unified Communications Server by completing the following steps:

Step 1 Navigate to **Configuration > Unified CM Settings**.

Step 2 In the Use Configuration TFTP Server area, click **Specify**.

Step 3 In the TFTP Server 1 area, specify the IP address of the Unified CM server.

Step 4 (Optional) If the system uses any additional Unified CM servers, specify those in the TFTP Server 2 through TFTP Server 4 area.

Step 5 Click **Apply**.

Configuring Your System After Initial Bootup

After successful bootup, the CTS Administration Software loads. When the CTS Administration software completes loading, the Cisco Unified IP phone displays a welcome message that shows the system IP address. The welcome screen only appears the first time the system is booted up after initial installation or after a factory reset.

Note The telephone displays a directory number of 7000, but the telephone is not yet registered and does not function.

Before You Begin

If you have not already done so, configure Cisco Unified Communications Manager. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

To continue your initial setup:

Step 1 From the CTS Cisco Unified IP phone welcome page, press **Next**. The system reboots.

Note The system might reboot several times during the initial startup process.

Step 2 Open a browser on a computer that is connected to the network.

Step 3 In the URL field, type in your IP address and press **Enter**. The browser launches the Cisco TelePresence System Administration interface.

Note If you need to obtain the IP address, complete the following steps:

a. On the CTS Cisco Unified IP phone, press the **Manual** softkey at the bottom of the screen.

b. Locate “Info” at the bottom of the screen and press the **Info** soft key.

c. Scroll down to the IP Address listing and copy the address.

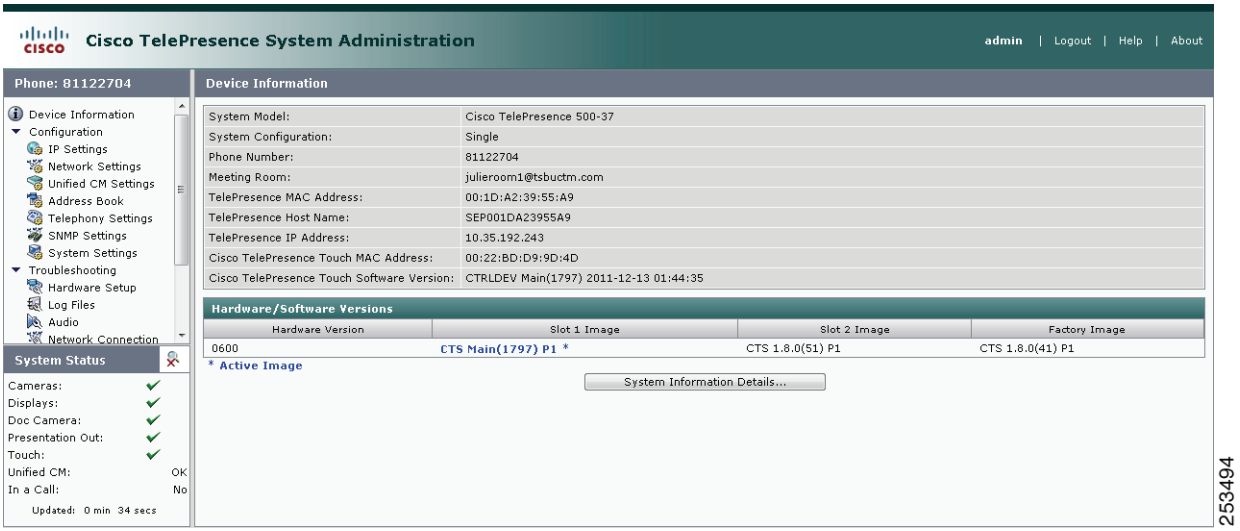
Step 4 Log in to the system by entering the following information:

- Username: **admin** (case sensitive)
- Password: **cisco** (case sensitive)

Note You can change your password in Unified CM. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Step 5 Click **Login**. The Device Information window appears, as shown in Figure 4-4.

Figure 4-4 Device Information Screen



Note See the "Upgrading CTS Codec Firmware" section on page 4-25 for information about upgrading to new CTS firmware releases.

Step 6 Continue to the following sections to configure your system:

- IP Settings, page 4-10
- Network Settings, page 4-12
- Cisco Unified Communications Manager Settings, page 4-13
- Address Book, page 4-15
- Telephony Settings, page 4-16
- SNMP Settings, page 4-18
- System Settings, page 4-20

IP Settings

The IP Settings window displays the Cisco TelePresence System (CTS) MAC address and hostname and you can view and manage the following:

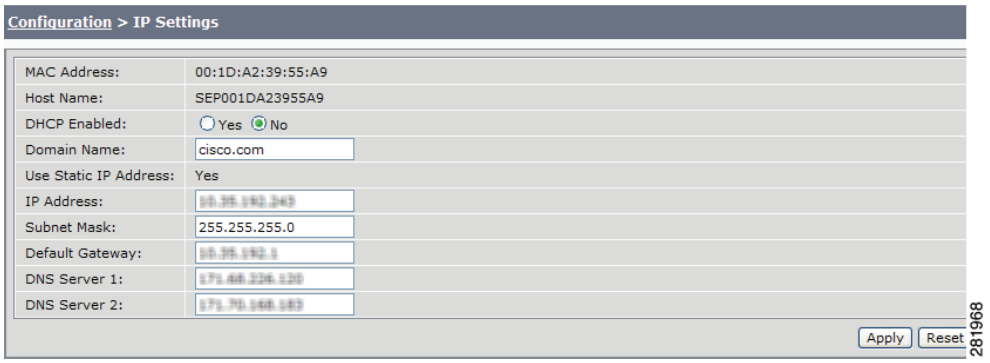
- DHCP—Select a static IP address, which allows the Cisco IP phone to be configured so that the system recognizes it as a device in the network, rather than a router.
- Domain name
- IP Address
- Default gateway
- DNS servers.

To view and manage IP settings:

Step 1 Choose **Configuration > IP Settings**. The IP Settings window appears, as shown in Figure 4-5 (DHCP Enabled) and Figure 4-5 (DHCP Not Enabled).

Figure 4-5 CTS IP Settings - DHCP Enabled

Figure 4-6 CTS IP Settings - DHCP Not Enabled



Step 2 Configure settings for the Cisco TelePresence System uplink to your network using the information in Table 4-1 as a guide. The Cisco TelePresence System can be configured in the following ways:

- Pure dynamic—Uses DHCP for everything.
- Pure static—Uses static settings for everything.

- Hybrid—Uses static settings for the IP Address, subnet mask and gateway, but uses DHCP for name servers and other options like Option 150 for the Unified CM TFTP servers.

Tip When you make a change in any of the **Configuration > IP Settings** fields, the **Apply** and **Reset** buttons are activated.

Step 3 Click **Apply** to register new or modified settings.

Step 4 Click **Reset** to restore the original settings.

Note All codecs on the system must be connected and enabled for the factory reset to complete. To register a device, see the "Optional Hardware" section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Table 4-1 IP Settings

Field or Button	Setting
MAC Address:	MAC address of the CTS primary codec. For example, " **00:0D:D1:23:45:A1** "
Host Name:	Host name of the CTS primary codec. For example, " **SEP000DD12345A1** "
DHCP Enabled:	Indicates whether Dynamic Host Configuration Protocol (DHCP) has been enabled for the CTS primary codec. • If you select the **No** radio button in the DHCP Enabled field, you can update the following available fields: – Domain Name – IP Address – Subnet Mask – Default Gateway – DNS Server 1 – DNS Server 2 • If you select the **Yes** radio button in the DHCP Enabled field, no configurable fields are available unless you click the **Yes** radio button to Use Static IP Address.
Domain Name:	Indicates the domain name for the primary codec. This field is configurable only if you select the **No** radio button for DHCP Enabled.
Use Static IP Address:	Indicates whether the CTS primary codec is configured to use a static IP address. Static IP address is disabled by default. Click the **Yes** radio button to update the following fields: • IP Address • Subnet Mask

Table 4-1 IP Settings

Field or Button	Setting
IP Address	IP address for the Cisco TelePresence system. This field is configurable only if you select the **No** radio button for DHCP Enabled.
Subnet Mask	Subnet mask used for the IP address supplied. This field is configurable only if you select the **No** radio button for DHCP Enabled.
Default Gateway	Default gateway for the CTS primary codec. This field is configurable only if you select the **No** radio button for DHCP Enabled.
DNS Server 1 and 2	IP addresses of the Domain Name System (DNS) servers. This field is configurable only if you select the **No** radio button for DHCP Enabled.

Network Settings

You can view or configure the following settings in the Network Settings window:

- Operational VLAN ID, page 4-12
- Administrative VLAN ID, page 4-13
- Syslog Address, page 4-13

Operational VLAN ID

This field shows a display-only VLAN ID that is standard for networks with a Cisco Unified IP phone.

Administrative VLAN ID

The CTS must have a VLAN membership ID before it can proceed with a DHCP request for an IP address.

To view or configure the administrative VLAN ID:

Step 1 Choose **Configuration > Network Settings**.

Step 2 Enter an administrative VLAN ID for Cisco TelePresence in this field.

Note The **Apply** and **Reset** buttons become active when a value is entered in this field.

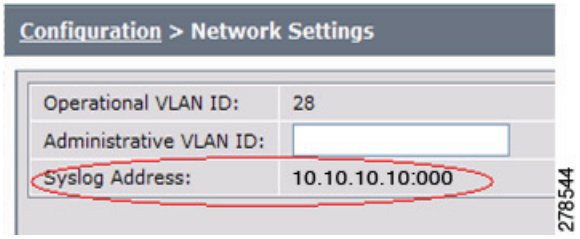
Step 3 Click **Apply** to register a new or modified setting.

Step 4 Click **Reset** to restore the administrative VLAN ID setting displayed when you opened this window.

Syslog Address

This field shows the display-only syslog address that is standard for networks with a Cisco Unified IP phone, as shown in Figure 4-7.

Figure 4-7 Network Settings Syslog Address



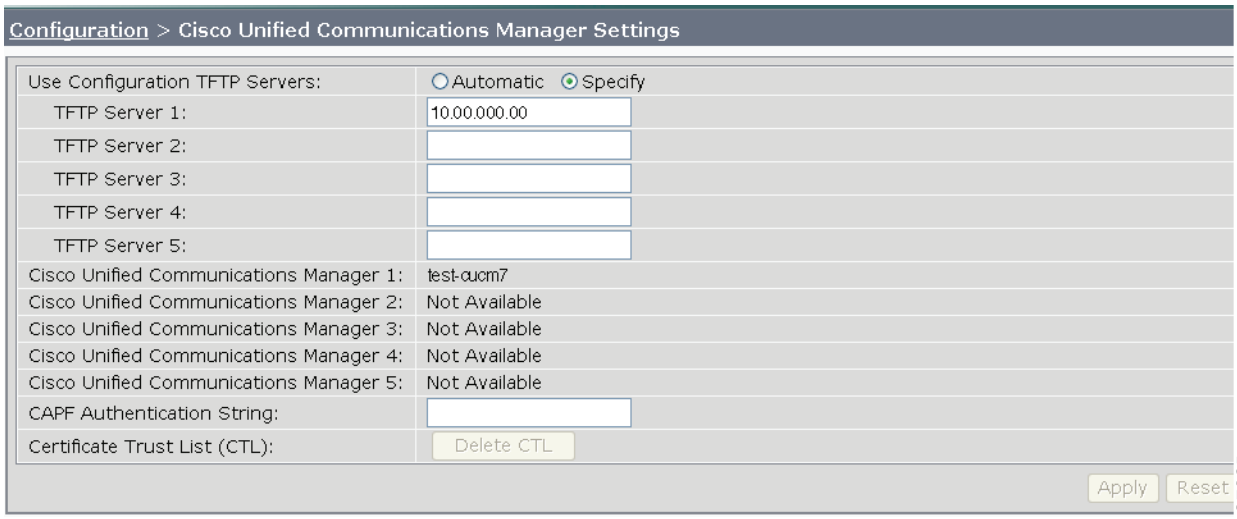
Note You must also configure the External Syslog Address in the Product Specific Configuration Layout field for your CTS. See the *Cisco Unified Communications Configuration Guide for the Cisco TelePresence System*.

Cisco Unified Communications Manager Settings

To specify TFTP server locations and view a list of available settings for this Cisco TelePresence system:

Step 1 Choose **Configuration > Cisco Unified Communications Manager Settings**. The Cisco Unified Communications Manager Settings window appears, as shown in Figure 4-8.

Figure 4-8 Cisco Unified Communications Manager Settings



Step 2 Configure Unified CM settings using the information in Table 4-2.

Note The **Apply** and **Reset** buttons become active when a value is entered in this field.

Table 4-2 Cisco Unified Communications Manager Settings

Field	Settings
Use Configuration TFTP Server	• Click **Automatic** to set the default condition, which is that the TFTP server will reply to DHCP requests for option 150, or for a list of TFTP servers that indicate to endpoints in the network where to find Unified CM configuration files. • Click **Specify** to manually supply IP addresses of TFTP servers in the interactive fields provided.
TFTP Server 1 through 5	Click **Specify** at Use Configuration TFTP Server to activate interactive fields that are provided for entering TFTP server IP addresses.
Cisco Unified Communications Manager 1 through 5	Display-only report that shows the names of up to five Cisco Unified Communications Managers.
CAPF Authentication String	Enter the Certificate Authority Proxy Function authentication string. The characters entered in this field must match the CAPF Authentication string entered in Unified CM.
Certificate Trust List (CTL)	The Delete CTL button becomes active when the CTS is provided with a CTL by a Unified CM configured in mixed authentication mode. Click **Delete CTL** to delete all entries on the CTL.

Step 3 Click **Apply** to register new or modified settings.

Step 4 Click **Reset** to restore the original settings.

Note All codecs on the system must be connected and enabled for the factory reset to complete. To register a device, see the "Optional Hardware" and "Troubleshooting the Cisco TelePresence Configuration" sections of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Related Information

See the following documentation for more information about Unified CM:

- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
- Cisco Unified Communications Manager (CallManager) Documentation Roadmaps

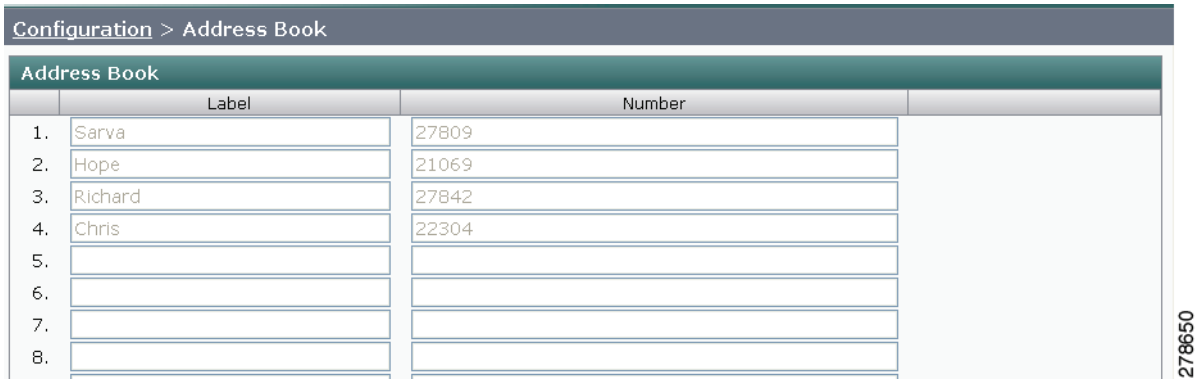
Address Book

The Address Book window displays read-only entries that have been set during Cisco Unified Communications Manager (Unified CM) configuration. You can create listings for up to 40 meeting rooms.

To view the phone list of Cisco TelePresence system-enabled meeting rooms:

Step 1 Choose **Configuration > Address Book**. The Address Book window appears, as shown in Figure 4-9.

Figure 4-9 CTS Address Book



Step 2 Use Unified CM to make changes to the Address Book. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

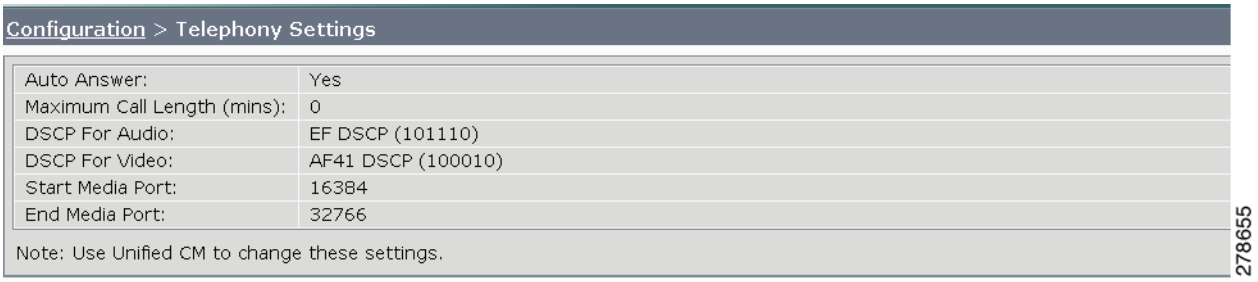
Telephony Settings

The Telephony Settings window displays read-only information about the telephony settings for the Cisco TelePresence System that were set in the Unified CM.

To view entries in the Telephony Settings window:

Step 1 Choose **Configuration > Telephony Settings**. The Telephony Settings window appears, as shown in

Figure 4-10 CTS Telephony Settings



Step 2 View the telephony settings described in Table 4-3.

Table 4-3 Telephony Settings

Field	Settings
Auto Answer	Displays the automatic answering capability on the phone. • **Yes** indicates that automatic answering has been enabled. • **No** indicates that automatic answering has been disabled.
Maximum Call Length (mins)	Displays the defined limit to the number of minutes allowed for a call. The default setting is 0 minutes, which means no limit to call duration is set. The maximum number of minutes that can be set is 10080 (7 days). The call will automatically end at the number of minutes set. When the default setting is used, the call is never ended automatically.

Table 4-3 Telephony Settings (continued)

Field	Settings
DSCP For Audio DSCP For Video	Displays the traffic queuing techniques that define per-hop behavior based on the Differentiated Services Code Point (DSCP) value in the IP header of a packet. The following DSCP settings apply for both audio and video traffic: • AF11 DSCP (001010) • AF12 DSCP (001100) • AF13 DSCP (001110) • AF21 DSCP (010010) • AF22 DSCP (010100) • AF23 DSCP (010110) • AF31 DSCP (011010) • AF32 DSCP (011100) • AF33 DSCP (011110) • AF41 DSCP (100010)—Recommended value • AF42 DSCP (100100) • AF43 DSCP (100110) • CS1 (precedence 1) DSCP (001000) • CS2 (precedence 2) DSCP (010000) • CS3 (precedence 3) DSCP (011000) • CS4 (precedence 4) DSCP (100000) • CS5 (precedence 5) DSCP (101000) • CS6 (precedence 6) DSCP (110000) • CS7 (precedence 7) DSCP (111000) • Default DSCP (000000) • EF DSCP (101110)
Start Media Port	Must be in the range from 16384 to 32766, and must be lower than the End Media Port settings.
End Media Port	Must be in the range from 16384 to 32766, and must be higher than the Start Media Port settings.

Step 3 Use Unified CM to make changes to Telephony Settings. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

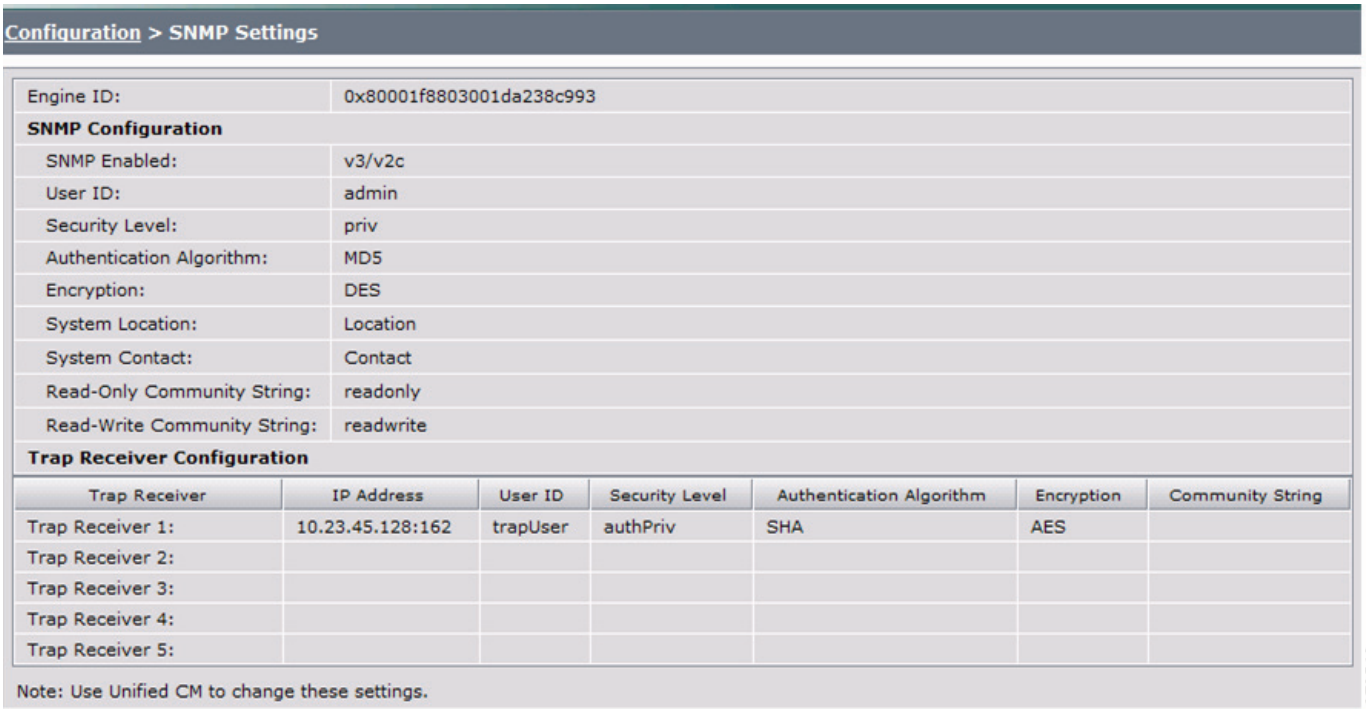
SNMP Settings

The Simple Network Management Protocol (SNMP) Settings window displays read-only information about the SNMP settings for the Cisco TelePresence System that were set in Unified CM configuration.

To view SNMP settings:

Step 1 Choose **Configuration > SNMP Settings**. The SNMP Settings window appears, as shown in Figure 4-11.

Figure 4-11 Verify SNMP Settings



Step 2 View the SNMP settings fields described in Table 4-4.

Table 4-4 SNMP Settings

Field	Settings
Engine ID	Identifies the local or remote SNMP engine. The remote agent SNMP engine ID and user password are used to compute authentication and privacy digests.
SNMP Configuration	Parameters that access the SNMP server associated with this Cisco TelePresence System. Unified CM for CTS supports SNMP Version 2c and Version 3. SNMP fields displayed in this window reflect the configured SNMP version. The following fields are included: • SNMP Enabled • User ID • Security Level • Authentication Algorithm • Encryption • System Location • System Contact • Read-Only Community String • Read-Write Community String
Trap Receiver Configuration	SNMP settings for the receiver to which this Cisco TelePresence system will send traps. The following information is shown for Traps 1 through 5: • Trap Receiver • IP Address • User ID • Security Level • Authentication Algorithm • Encryption • Community String

Step 3 Use Unified CM to make changes to the SNMP settings. For more information, refer to the "SNMP Configuration Parameters Area" and "SNMP Trap Parameters Area" sections of the "Configuring Cisco Unified Communications Manager for the Cisco TelePresence System" chapter in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Related Information

For more information about configuring SNMP with your Cisco TelePresence system, refer to the "MIBs, RFCs, and SNMP Trap Messages for the Cisco TelePresence System" chapter of the *Cisco TelePresence System Message Guide*.

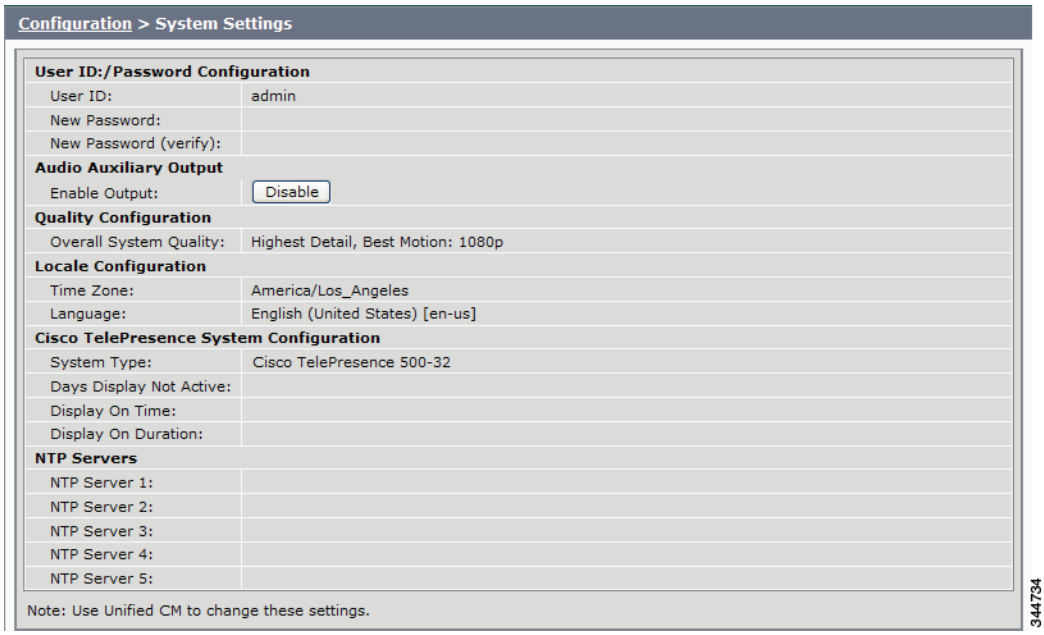
System Settings

The System Settings window displays read-only information about the system settings for the Cisco TelePresence System that were set in Unified CM configuration.

To view system settings:

Step 1 Choose **Configuration > System Settings**. The System Settings window appears, as shown in Figure 4-12.

Figure 4-12 CTS System Settings



Step 2 View the system settings information described in Table 4-5.

Table 4-5 System Settings

Field	Description or Setting
Username/Password Configuration	
User ID New Password New Password (verify)	Displays username and password. **Note** Usernames and passwords must be at least 4 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.
Audio Auxiliary Output	

Table 4-5 System Settings (continued)

Field	Description or Setting
Quality Configuration	
Overall System Quality	This field displays the system bandwidth and screen resolution. The bandwidth is the maximum negotiated video bandwidth for a CTS call. A higher bandwidth increases video quality. Choose from the following: • Highest Detail, Best Motion: 4Mbps 1080p (default) • Highest Detail, Better Motion: 3.5Mbps, 1080p • Highest Detail, Good Motion: 3Mbps, 1080p • High Detail, Best Motion: 3Mbps, 720p • High Detail, Better Motion: 2Mbps, 720p • High Detail, Good Motion: 1Mbps, 720p • High Detail, Limited Motion: 720p (Lite)
Locale Configuration	
Time Zone	Displays the configured time zone for your area of the world from the drop-down menu.
Language	Displays the configured language for CTS. **Note** CTS software releases starting with Release 1.10 support additional languages. These languages change the text that is shown on the Cisco TelePresence Touch 12 device and also affect some on-screen messages. For more information, refer to the "Installing Language Versions" section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.
Cisco TelePresence System Configuration	
System Type	Identifies the CTS model. You must select the CTS device type from the list to upgrade your CTS software.
Days Display Not Active	Specifies the days of the week that the Cisco TelePresence system display remains off by default. Choose Monday through Sunday. Default is Sunday and Saturday.
Display On Time	Specifies the time of day that the Cisco TelePresence system display(s) will remain on after being turned on, if CCM is configured. Times are displayed in a 24-hour format where 00:00 indicates 12:00 midnight and 23:59 indicates 11:59 pm. Default is 07:30. If you clear the default value so that the field is blank, the display(s) will turn off after the completion of each call.
Display On Duration	Specifies the length of time the Cisco TelePresence system display(s) will remain on if a "Display On Time" value is defined. Times are displayed in a 24-hour format, where 1:30 indicates one hour and thirty minutes; the maximum value is 24:00 (24 hours). Default is 10:30. If you clear the default value so that the field is blank, then the display will turn off at 11:59 pm.

Table 4-5 System Settings (continued)

Field	Description or Setting
Note If your version of Unified CM does not allow you to configure values for Days Display Not Active, Display On Time or Display On Duration, the system uses the default values for these features.	
NTP Servers	
NTP Server 1 through 5	Required. Network Time Protocol (NTP) is used to synchronize the clocks on Cisco IP telephony servers with an external network time server that uses NTP. You can have up to five IP addresses for Network Time Protocol servers. **Note** NTP must be configured properly to ensure that calendar events appear as expected.

Step 3 Use Unified CM to make changes to the system settings. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for more information.

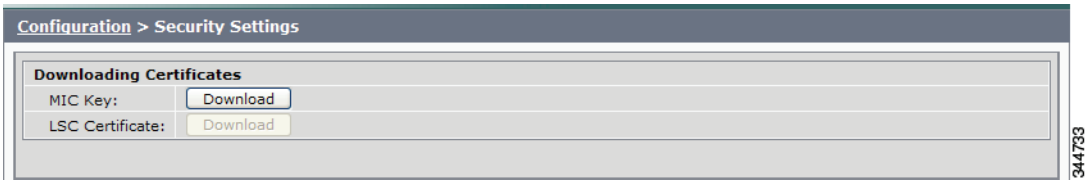
Security Settings

The Security Settings window enables you to download a Manufacturing Installed Certificate (MIC) key or Locally Significant Certificate (LSC) certificate for 802.1X authentication. For more information about 802.1X authentication, see "Configuring Your System for 802.1X Authentication" section on page 4-28.

To download a MIC key or LSC certificate:

Step 1 Choose **Configuration > Security Settings**. The Security Settings window appears, as shown in Figure 4-13.

Figure 4-13 Security Settings



Step 2 To download a certificate, click the Download button next to it.

Note If a certificate is not present in the system, the Download button next to it is dimmed.

Step 3 Save the certificate to your hard disk.

Troubleshooting Your Configuration

Use the information in Table 4-6 to help you troubleshoot your configuration.

Before You Begin

First check that the following conditions have been met:

- Power has been applied.
- The Cisco TelePresence System has been installed and configured according to the instructions in Cisco TelePresence System Assembly Guides.
- Unified CM has been configured to support the Cisco TelePresence System as described in the *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System.*

Table 4-6 Troubleshooting the Cisco TelePresence Configuration

Problem	Possible Cause	Possible Solutions
Selecting the Test Connection function on the Unified CM web page results in an error.	Incorrect Cisco TelePresence Manager Application User credentials: • Cisco TelePresence Manager Application User is missing required roles.	1. **Check User Credentials**—Correct the user credentials. 2. **Check Cisco TelePresence Manager Application**—See the Cisco TelePresence Manager documentation home page for information about using the Cisco TelePresence Manager.
The Cisco TelePresence unit does not register.	Cisco TelePresence System could be unknown: • Unified CM does not know about the CTS. • CTS is not registered because it is unplugged. • CTS MAC address is entered incorrectly.	1. **Test Codec Connection**—Test the network connection to the master codec by plugging the codec network cable directly into the IP phone. If the IP address displays, the problem is with the codec. 2. **Verify Phone Registration**—Log in to the Unified CM administration interface. Click the IP address and verify phone registration.
The Cisco Unified IP Phone 7975 does not register.	Phone could be unknown: • Unified CM does not know about it. • CTS is not registered because it is unplugged. • CTS MAC address is entered incorrectly. • The incorrect device type was configured in Unified CM.	**Verify Phone Registration**—Log in to the Unified CM administration interface. Click the IP address and verify phone registration. • Confirm that a 7970 or 7975 respectively, device type has been configured in Unified CM.

Table 4-6 Troubleshooting the Cisco TelePresence Configuration

Problem	Possible Cause	Possible Solutions
The phone does not display the Cisco TelePresence idle screen.	• Phone could be unknown: – Unified CM does not know about it – CTS is not registered because it is unplugged. – The phone did not receive an IP address. • There could be errors in the Cisco Unified Communications Manager Phone Configuration window: – Incorrect IP address – Typos in the external location URLs	1. **Verify Phone Registration**—Log in to the Unified CM administration interface. Click the IP address and verify phone registration. 2. **Verify Phone in the System**—Log in to the Cisco TelePresence System Administration interface verify that the system can detect the phone. 3. **Correct Typos in URL**—See "Managing Cisco Unified IP Phones" in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for information about configuring external URLs.
CTS does not auto answer	• An incoming conference call is ringing and the CTS does not auto answer immediately. • The call is connected but there is no video	The CTS rings and auto-answers a call based on how these features were configured in Unified CM. If the call is connected as audio only, check your IP phone configuration and make sure the "Disable Speaker/Headset" box is checked. To disable the IP phone speaker/headset: 1. Logon to the CUCM 2. Search for your directory number (DN). Two devices are displayed: CTS and Cisco Unified IP Phone. 3. Click the IP_Phone device. 4. Scroll down to the Product Specific Configuration Layout window. 5. Verify that the following check-boxes are checked in the Product Specific Configuration Layout window: – Disable Speakerphone – Disable Speakerphone and Headset 6. Apply and Save the configuration. 7. Reset the device. See the *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System* for more information.

Table 4-6 Troubleshooting the Cisco TelePresence Configuration

Problem	Possible Cause	Possible Solutions
Call terminates prematurely	DSP failure due to incompatible CTS software version.	CTS devices are backward compatible up to two CTS Software Releases. You may want to upgrade your software.
• Conference room is deleted from future meeting schedule in CTS Manager. • Lost ability to invite expected conference room into a call. • Studio Mode recording is not working. • SD InterOp feature is not working. • HD InterOp feature is not working.	The Cisco TelePresence Recording Server (CTRS) Studio Mode recording feature is not working and the room has been unsubscribed. One or more of the rooms in a conference does not support the feature.	Check Room View on CTS-Man to verify whether a CTS device is capable of supporting the features in a specific room. Then check your Unified CM configuration settings to configure the device. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for more information.

Upgrading CTS Codec Firmware

Note Upgrades should only be performed at night or during minimal Cisco TelePresence usage times. An upgrade takes up to 30 minutes to complete.

The procedure to upgrade CTS firmware is the same as the firmware upgrade procedure for the Cisco Unified CM IP phones. See the Uploading Files to the Cisco Unified CM TFTP Directory section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for complete instructions.

To download CTS firmware:

Step 1 Log into the Download Software Select a Product page on Cisco.com:

http://www.cisco.com/cisco/software/navigator.html

The Tools & Resources Download Software appears.

Step 2 Expand the **Cisco TelePresence System** folder and open the **Cisco TelePresence System** sub folder. A list of CTS devices appears.

Step 3 Select your CTS device

Step 4 Upload the firmware file to the TFTP directory of your Unified CM TFTP server.

Step 5 Restart the TFTP server.

Step 6 Change the firmware filename for the system(s) that you want to upgrade (either via the Device Defaults page, or on a per system basis) in the Cisco Unified CM Administration interface.

Step 7 Click the **Restart** button in Unified CM for the device(s) that you want to upgrade.

Upgrading Software for Cisco TelePresence Touch 12

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

Managing Passwords

This section contains the following information about managing and troubleshooting password issues on the Cisco TelePresence System (CTS):

Resetting Your CTS Codec Password

Note You must be in the Cisco TelePresence room to read the newly requested passcode that shows on the main display.

At each point where the **pwrecovery** account requires input, the program will wait up to 60 seconds. If nothing is entered, the system will inform you that the entry took too long and will exit.

If you encounter any difficulty, open a case with Technical Assistance Center (TAC) via the Internet at http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered about the problem.

Before You Begin

Make sure that the CTS is not in a call, and that there is only one instance of someone trying to reset the password, otherwise the session will abort.

Procedure

To reset your CTS codec password:

Step 1 SSH into the codec from your laptop.

Step 2 Login with the following:

- Username: **pwrecovery**
- Password: **pwreset**

The following message appears in the SSH client window:

Example 4-1 Welcome to Password Reset

```
dhcp-249:~ $ ssh pwrecovery@10.00.00.100
pwrecovery@10.00.00.100's password:

*********************************************
*********************************************
**                                         **
**      Welcome to password reset           **
**                                         **
*********************************************
*********************************************

Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:
```

Step 3 The system will ask whether you want to continue. Type **Y** then **return** to continue

Note If desired, type any other key then **return** to exit.

This system will now prepare for password reset and prompt you for a passcode. The new passcode is displayed on the CTS main display, as shown in the following example:

Password reset is now being run

Passcode: 919175

Note The passcode is a randomly generated number and will be different for each login attempt. If you enter the wrong passcode, the system will inform you that the passcode was incorrect and will exit, as shown in the following example. If this happens, repeat Step 1 and Step 2.

Example 4-2 Invalid Password Reset Request

```
Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:12345
Sorry that was an invalid passcode...
Logging off
Connection to 10.00.00.100 closed.
dhcp-249:~ $
```

When you enter the correct passcode, the CTS will then reset the administration account name and password to the system defaults. The following example shows successful password reset information:

Example 4-3 Successful Password Reset Request

```
Please enter the passcode:507530
resetting admin name and password
stopping any existing admin session
admin account and password reset to default
success in applying security rules
Logging off
Connection to 10.00.00.100 closed.
dhcp-249:~ $
```

Note If you are using the CTS with a Cisco Unified Communications Manager, the next time you perform a "Refresh" or "Reset" from the Unified CM, the administration account name and password will be reconfigured to the values specified in the Unified CM device page.

Configuring Your System for 802.1X Authentication

This chapter describes how to set up, monitor, and troubleshoot 802.1X authentication in the Cisco TelePresence System:

IEEE 802.1X Authentication Overview

802.1X is an IEEE standard for port-based network access control. It offers the capability to permit or deny network connectivity, control Virtual LAN (VLAN) access, and apply traffic policy, based on user or machine identity.

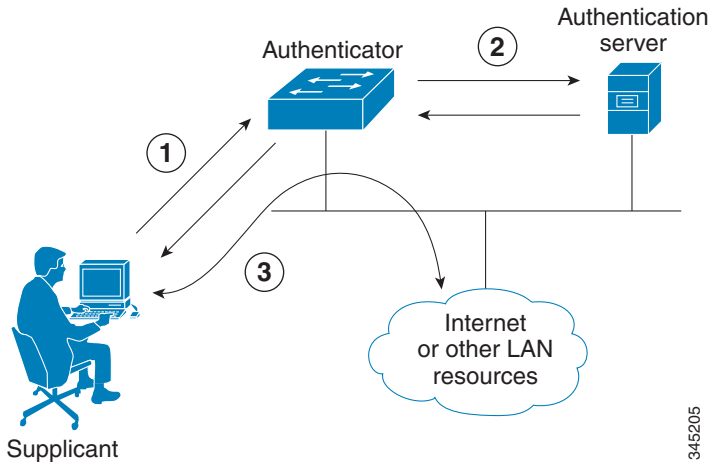
802.1X permits or denies device access to the network by using authentication. Ethernet switch ports can be enabled dynamically based on the identity of the device that connects to it. Devices which are not authenticated cannot gain access to the network.

802.1X Authentication Components

802.1X authentication involves the following three network devices:

- A **supplicant**: a client device (such as a laptop or endpoint) that attempts to access a LAN/Wireless LAN (WLAN), or the software that runs on this device and that provides credentials to the authenticator.
- An **authenticator**: a network device (such as an Ethernet switch or wireless access point) that acts as an access point to a protected network. For 802.1X authentication, the supplicant provides network credentials, such as user name, password, digital security certificate, or a combination of these, to the authenticator. The authenticator then forwards the credentials to the authentication server for verification.
- An **authentication server**: a server (such as Cisco Secure Access Control Server) that guards the protected network. For 802.1X authentication, the authentication server receives the supplicant's network credentials from the authenticator and verifies the supplicant's identity. Then the supplicant is able to access the resources located on the network.

Figure 4-14 Diagram of 802.1X Authentication Process



Authenticating Your System

Your Cisco TelePresence System is equipped to function as an 802.1X-compliant supplicant. 802.1X authentication is enabled by default.

Note Cisco recommends that you configure your switch port (or authenticator) for multi-domain mode.

Setting up 802.1X Authentication

This section describes the steps you perform to set up 802.1x authentication, and includes the following topics:

- Authenticating the Cisco TelePresence System Using a Security Certificate (MIC or LSC), page 4-30
- Examining the Security Certificate in the Cisco TelePresence System, page 4-30

Note In order to complete 802.1X authentication, you must use a port that is not already enabled for 802.1X.

Authenticating the Cisco TelePresence System Using a Security Certificate (MIC or LSC)

When the Cisco TelePresence System receives an authentication challenge from an Authenticator, the system responds with either the Manufacturing Installed Certificate (MIC) or the Locally Significant Certificate (LSC). When both the MIC and LSC are installed, the system uses the LSC to authenticate. If the LSC is not installed, Cisco TelePresence System uses the MIC, as the MIC is built into the system by the manufacturer.

The LSC provides greater security because it creates a public key infrastructure (PKI) that is unique to each system. To authenticate the codec using the LSC, you must install it on your system manually by using the Certificate Authority Proxy Function (CAPF) in Cisco Unified Communication Manager (CUCM). For more information, see the "Installing the LSC" section on page 4-30.

Installing the LSC

To install the LSC, refer to the "Deploying Locally Significant Certificates" section found in the *IP Telephony for 802.1X Design Guide*.

Examining the Security Certificate in the Cisco TelePresence System

You may want to examine the security certificate (MIC or LSC) on an 802.1X-authenticated system in order to verify that the certificates are valid, not expired, and issued by the CAPF.

To examine the security certificate in your Cisco TelePresence System, you may download a copy of the certificate to your own system by using either of two methods:

- Downloading the Security Certificate Using the CLI, page 4-30
- Downloading the Security Certificate Using the GUI, page 4-31

Downloading the Security Certificate Using the CLI

To download the MIC or LSC using the CLI, complete the following steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command: **file get cert** {*cert-type*} {*SCP-user*} {*SCP-password*} {*IP-address-or-hostname*} {*file-save-location*}

See Table 4-7 for syntax descriptions.

Table 4-7 Syntax Descriptions

Argument	Description
cert-type	Type of certificate to retrieve (either MIC or LSC)
SCP-user	Username of Secure Copy (SCP) user
SCP-password	Password for SCP user
IP-address-or-hostname	Hostname or IP address of target system
file-save-location	Location to save file on target system

After entering the command, the security certificate will save on the target system in the designated file-save location:

```
file get cert MIC username password 10.1.1.1 /home/user
Uploading MIC to 10.1.1.1...DONE
```

If you select the LSC as the type of certificate to retrieve, but the LSC is not installed on the Cisco TelePresence System, the command line will read as follows:

```
admin:file get cert LSC username password 10.1.1.1 /home/user
Uploading LSC to 10.1.1.1...LSC does not exist
Executed command unsuccessfully
```

If the LSC command is unsuccessful, you need to install the LSC on the codec. See the "Installing the LSC" section on page 4-30. If the command is successful, continue to the next step.

Step 3 Go to the designated file-save location, and click the file to view the certificate.

Downloading the Security Certificate Using the GUI

To download the MIC/LSC from the GUI, complete the following steps:

Step 1 Log into the GUI and navigate to **Configuration > Security Settings.**

Step 2 Click **Download** to download and view a certificate. A dimmed Download button indicates the lack of a given certificate.

Checking the CTS 802.1x Authentication Status

To check 802.1X authentication status in the Cisco TelePresence System, use either of the following options:

- View the CTS primary display screen during system bootup (see the "Checking the 802.1X Authentication Status on the Primary Display Screen" section on page 4-32)
- Enter the CLI command **show dot1x status** (see the "Checking the 802.1X Authentication Status with a CLI Command" section on page 4-33)

Checking the 802.1X Authentication Status on the Primary Display Screen

To check the 802.1X authentication status on the Cisco TelePresence System primary display screen, complete the following steps:

Step 1 Power off the Cisco TelePresence System.

Step 2 Power on the Cisco TelePresence System.

Step 3 View the bottom right of the primary display screen. In a three-screen system, view the bottom-right of the center screen. Text will display to indicate whether 802.1X is authenticated, not authenticated, or not required on your system.

Example:

```
802.1X: Connecting...
802.1X: Not Authenticated
```

This text, as viewed on the Cisco TelePresence System primary display screen, indicates the success or failure of 802.1X authentication on that system. If the status line reads "Not Required," 802.1X authentication is not required for that system.

Figure 4-15 Screenshot of Cisco TelePresence System Boot-Up Screen

See Table 4-8 for a summary of 802.1X authentication status displays for enabled and non-enabled networks.

Table 4-8 802.1X Authentication Status Display Summary

Status	802.1X-Enabled Network	Non-802.1X-Enabled Network
In Progress	Connecting / Authenticating	Connecting
Success	Authenticated	Not Required
Failure	Not Authenticated	Not Required

Note The 802.1X authentication status can only be viewed on your Cisco TelePresence System primary screen, not on a secondary screen (e.g., a presentation screen, or in a three-screen system, the left or right screen). If the 802.1X authentication status does not show on the primary screen, follow the steps below listed under the "Checking the 802.1X Authentication Status with a CLI Command" section on page 4-33

Checking the 802.1X Authentication Status with a CLI Command

To check the 802.1X authentication status with a CLI command, complete the following steps:

Step 1 Log into the CLI.

Step 2 Input the following command: **show dot1x status**

Step 3 View resulting text. Text will display indicating whether 802.1X is authenticated, not authenticated, or not required on your system.

Example:

```
admin:show dot1x status
Authenticated
```

Troubleshooting 802.1x Authentication Issues

When 802.1X does not authenticate properly, review the following sections:

- Troubleshooting Issues in 802.1X Authentication, page 4-33
- Viewing the Security Certificate, page 4-35

Troubleshooting Issues in 802.1X Authentication

Table 4-9 summarizes some issues that may appear during 802.1X authentication, as well as potential resolutions.

Table 4-9 Troubleshooting Issues in 802.1X Authentication

Symptom	Possible Root Causes	Resolution
Cisco Secure ACS authentication server rejects security certificate from the Cisco TelePresence System supplicant.	The security certificate is invalid, expired, or not issued by CAPF.	Install a valid, non-expired security certificate using the CAPF. See Viewing the Security Certificate.
Cisco TelePresence System fails 802.1X authentication.	Errors may be present in the system's most recent log files.	Use the **file list log dot1x** command in the CLI to check logs for error or failure messages.
Cisco TelePresence System displays "802.1X: Not Required" on its boot-up screen.	The ethernet switch is not configured to support 802.1X.	Check the 802.1X authentication status on the ethernet switch by logging into the switch and using the CLI command **show authentication sessions interface** {**FastEthernet** | **GigabitEthernet**} {*Interface Number*}. If the ethernet switch is not 802.1X-enabled, enable it. Please refer to *Identity-Based Networking Services: IP Telephony in IEEE 802.1X-Enabled Networks Deployment and Configuration Guide* for instructions.
Cisco Secure ACS authentication server rejects security certificate from the Cisco TelePresence System supplicant.	Cisco Secure ACS is not configured to support 802.1X.	Configure Cisco Secure ACS (and all backend network configurations) to support 802.1X. Please refer to *Identity-Based Networking Services: IP Telephony in IEEE 802.1X-Enabled Networks Deployment and Configuration Guide* for instructions.
Cisco TelePresence System attempts authentication with the MIC instead of the LSC.	The LSC has not been exported from CAPF and imported into Cisco Secure ACS.	Check that the LSC is exported from CAPF and imported into Cisco Secure ACS. See Installing the LSC.
After moving to a different CAPF and Unified CM, Cisco TelePresence System fails 802.1X authentication.	The LSC no longer supports 802.1X authentication, since it was installed from the previous CAPF and Unified CM. Moving the Cisco TelePresence System to a different CAPF and Unified CM requires reinstalling the LSC and upgrading the system.	Reinstall the LSC from Cisco Unified CM and upgrade the Cisco TelePresence System. See Installing the LSC.

Viewing the Security Certificate

You may need to examine the security certificate (MIC or LSC) in order to verify that the certificates are valid, not expired, and issued by the CAPF.

You can use the CLI or a third-party tool to view the MIC or LSC.

- Viewing the Security Certificate from the CLI, page 4-35
- Viewing the Security Certificate from a Third-Party Tool, page 4-35

Viewing the Security Certificate from the CLI

To show the MIC or LSC from the CLI, complete the following steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command: **show cert** {**mic** | **lsc**}. You must enter either **mic** or **lsc**, not both.

Step 3 View the certificate that displays within the CLI. Verify that the certificate is valid, not expired, and issued by the CAPF.

Example:

```
> admin:show cert lsc
> Certificate:
Data:
Version: 3 (0x2)
Serial Number: 5 (0x5)
Signature Algorithm( sha1WithRSAEncryption
Issuer: C=US, O=organization, OU=department, CN=CAPF-1a234bcd, ST=CA, L=CH
Validity
Not Before: Mar 23 16:10:31 2012 GMT
Not After: Mar 22 16:10:30 2017 GMT
Subject: C=US, O=organization, OU=department, CN=SEPXXXXXXXXXXXX
```

If you enter **show cert lsc** on a system where the LSC is not installed, the command line will read as follows:

```
show cert lsc
There is no certificate to display
```

If the security certificate is expired, invalid, or issued by a different source, install a new certificate using the CAPF.

Viewing the Security Certificate from a Third-Party Tool

You can also view the MIC or LSC using a third-party tool. Consult the documentation provided with the tool for instructions.

Monitoring the Cisco TelePresence System

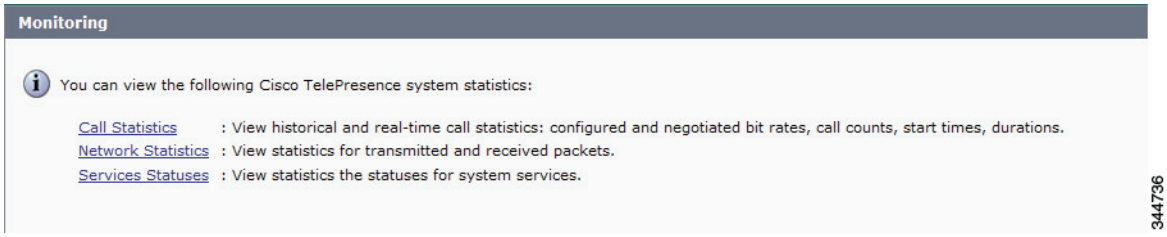
Created: April 2013, OL-28614-01

Contents

This chapter contains the following sections:

Figure 5-1 shows the tools that are available in the Monitoring window:

Figure 5-1 Monitoring Window



Call Statistics

See the "Call Statistics" section on page 2-14 for more information about this field.

Network Statistics

See the "Network Statistics" section on page 2-17 for more information about this field.

Services Statuses

See the "Services Statuses" section on page 2-18 for information about this field.

Using SNMP Traps to Monitor the Cisco TelePresence System

Cisco provides you with management information bases (MIB) files that are designed to monitor your system using the Simple Network Management Protocol (SNMP). For more information, refer to the "MIBs, RFCs, and SNMP Trap Messages for the Cisco TelePresence System" chapter of the *Cisco TelePresence System Message Guide*.

Where to Go Next

For more information about system statistics and messages, including System Operations (Sysop) Log messages see the *Cisco TelePresence System Message Guide* on Cisco.com.

Satellite Licenses for the Cisco TelePresence System

Created: April 2013, OL-28614-01

Contents

The information in this appendix explains how to order satellite licenses and how to configure both Cisco Unified Communications Manager (Unified CM) and Cisco TelePresence System (CTS) to support satellite functionality. This appendix contains the following sections:

Cisco TelePresence over Satellite Networks

The Cisco TelePresence over Satellite Networks solution extends the reach of Cisco TelePresence to remote, tactical locations where terrestrial bandwidth is not available. This solution incorporates existing Cisco TelePresence endpoint and infrastructure products with new software releases designed to function more effectively on poor, high-delay networks.

The following features and benefits are supported:

- Relaxed latency, jitter, and packet-loss thresholds allow the Cisco TelePresence meeting application to function effectively over poor, high-delay, real-world satellite networks.
- Qualification and testing of Type 1 encryption devices with the Cisco TelePresence application enable military-grade security for Cisco TelePresence calls.
- New network and environment recommendations provide guidance for remote, tactical, and even mobile deployments of the Cisco TelePresence System (CTS).

This section contains the following information:

Supported CTS Devices

The CTS 1000, CTS 1100, CTS 1300, and CTS 500 endpoint models are supported as the remote endpoint on the far end of a satellite link.

Other endpoint models (CTS 3000 and CTS 3200) have not been qualified to work on the remote side of a satellite link because the bandwidth needed for these three-screen systems quickly becomes cost-prohibitive to run over satellite networks. Any Cisco TelePresence endpoint or mix of endpoints (for a multipoint call) can be used on the terrestrial side of the satellite link.

Supported CTS Software

You must be running CTS software version 1.5 or a later release on all Cisco TelePresence endpoints, Cisco TelePresence Multipoint Switches, and Cisco TelePresence Managers within your network to participate in a satellite call.

Supported Satellite Bandwidth

You will need a minimum of 3-MB bandwidth (at 720p, good motion handling) in a single-channel-per-carrier (SCPC) configuration over a single-hop satellite link.

Note Because the Cisco TelePresence video and audio are traveling up to the satellite and back down to an earth station, significant (500 ms or more) latency is introduced into the signal. The result is noticeable delay in the conversation. In addition, atmospheric conditions or other interference may impact satellite-link performance and introduce jitter or packet loss into the call. The result may be noticeable degradation of the video quality.

CTS software release 1.5 and later releases support satellite deployment configurations that significantly raise the thresholds for network warning messages and call termination. When a satellite endpoint joins a call (point-to-point or multipoint), all other endpoints in the call negotiate the new threshold setting, so no one in the call gets warning messages or gets dropped just because a satellite-based endpoint joins the call.

Satellite Security

The Cisco TelePresence application supports Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) encryption for signaling and media paths.

Ordering a Satellite License

You can order satellite licenses when you initially order your CTS, or you can purchase separate satellite licenses to upgrade an existing CTS. Note the following details when you order a satellite license:

- The product authorization key (PAK) will either be physically delivered to your location or electronically delivered via E-mail.
- Product Number:
  - Physical: CTS-SATELLITE=
  - Electronic: L-CTS-SATELLITE=

Loading a Satellite License

After you have received the satellite license, load it on Unified CM by following these steps:

Caution Do not edit or change the contents of the license or it will become invalid.

Step 1 Load the license file into the Cisco Unified CM TFTP directory by following the steps in the "Uploading Files to the Cisco Unified CM TFTP Directory" in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Step 2 After making sure that the license is available on your computer, log in to the Cisco Unified CM Administration page and follow these steps:

a. From the Navigation drop-down menu in the upper right corner, select **Cisco Unified OS Administration** and click **Go**.

b. Log in to Cisco Unified OS Administration.

c. From the Software Upgrades drop-down menu, select **TFTP File Management** and click the **Upload File** button. A dialog box appears.

d. Browse to find the appropriate license and upload the license. Leave the Directory field blank.

Step 3 Restart the Cisco Unified CM TFTP server and complete these steps:

a. From the Navigation drop-down menu, select **Cisco Unified Serviceability** and click **Go.**

b. Log into Cisco Unified Serviceability.

c. From the Tools drop-down menu, select **Control Center - Feature Services**.

d. In the Select Server box, select the TFTP server from the drop-down menu and click **Go**.

e. In the CM Services box, select the **Cisco TFTP** radio button.

f. Click **Restart**.

g. Repeat Step c through Step e for all TFTP servers.

Identifying the CTS Satellite Endpoints

After you have loaded the satellite license on Unified CM, identify the CTS satellite endpoints so that they can retrieve the satellite licenses.

To identify the CTS satellite endpoints using the Cisco Unified CM Administration interface:

Step 1 Log in to the Cisco Unified CM Administration page.

Step 2 From the Device drop-down menu, select **Phone**.

Step 3 Using the Find search fields, locate the CTS that will be used as a satellite endpoint.

Step 4 Click **Reset** to bring up a new dialog box, and then click **Restart**.

Step 5 Repeat Step 2 through Step 4 for each CTS satellite endpoint.

Enabling the Satellite Feature

After the satellite license has been loaded on Unified CM, and the CTS satellite endpoints have been identified, you are ready to enable the satellite feature using CTS command-line interface (CLI) commands. For information about using CTS CLI commands, see the *Cisco TelePresence System Command-Line Interface Reference Guide*.

To enable the satellite feature:

Step 1 Check to see that the satellite license is available. From the CTS CLI admin command prompt, enter the following command:

```
admin:show license status

License feature status
satellite:
  Valid license found
  License feature is disabled
  Feature is currently not running
```

Step 2 Enable the satellite feature using the following command:

```
admin:set license satellite enable

License for satellite feature changed to enabled
```

Step 3 Restart the calling services using the following command:

```
admin:utils service restart Calling

Calling_Services   Restarting...done
```

Additional Licensing Information

See the Cisco TelePresence Administration Software Licensing Information page on Cisco.com.

A

ACU Auxiliary Control Unit. Provides the ability to conserve energy by powering the lights, presentation display, and optional peripherals for Cisco TelePresence systems on and off.

ad hoc meeting Non-scheduled, administrator-initiated, dial-out meeting. A meeting scheduler or administrator initiates the meeting through the Cisco TelePresence Multipoint Switch (CTMS) administration interface by listing the telephone number of the rooms which will participate in the multipoint meeting. See static meeting.

Auto Answer A phone set to automatically answer an inbound call. Use the Auto Answer feature in Cisco Unified Communications Manager. Activating this option or button causes the speaker phone to go off hook automatically when an incoming call is received.

Auto Collaborate Cisco TelePresence supports simple information sharing using a powerful "Auto Collaborate" feature that allows any object, document, or PC application to be displayed in a plug-and-play fashion. Auto Collaborate enables you to share images instantly in multiple locations by plugging in a laptop computer or high-definition ceiling document camera. The Cisco TelePresence 3000 Series built-in projector automatically displays images from the most recently activated device.

Ceiling cameras are perfect for capturing images of objects that are too valuable to ship, or cannot easily be copied or sent electronically. Cisco recommends and supports document cameras made by WolfVision, specifically the WolfVision Visualizer. This is a special live-camera system designed for picking up any object on a working surface with perfect illumination and depth of focus. All types of objects (e.g., photos, books, brochures, transparencies, slides, or three-dimensional objects) can be picked up quickly and easily, and meeting participants can use a wireless remote to control light, zoom, or focus.

Cisco TelePresence 3000 and 1000 systems support the Auto Collaborate capability, and meeting organizers can project content in multiple locations, including above or below displays, or on the side of a room.

A/V Expansion Box Audio/video extension unit. Required if your system uses an Auxiliary Control Unit (ACU).

B

bit rate Speed at which bits are transmitted, usually expressed in bits per second.

black screen codes System status information messages that appear on the main display screen before your meeting starts and while the screen is still black. For example, "Please wait, you are the first meeting participant."

For more information, see the *Cisco TelePresence System User Guide*.

C

call control device External device that controls the Cisco TelePresence System: Cisco Unified IP Phone, and the Cisco TelePresence Touch.

CCP The Conference Control Protocol (CCP) is an interface between the CTS and the CTMS that controls the elements of a Cisco TelePresence meeting.

CIF Common Intermediate Format. A video standard that provides 352x288 pixels, or picture elements, of video resolution.

Cisco CTI Manager CTI Manager is required in a cluster for applications that use TAPI or JTAPI Computer Telephony Integration (CTI). The CTI Manager acts as a broker between the CTI application and the Cisco Unified Communications Manager Service. It provides authentication of the application and enables control or monitoring of authorized devices. The CTI application communicates with a primary CTI Manager and, in the event of a failure, will switch to a backup CTI Manager. The CTI Manager should be enabled only on call processing subscribers, thus allowing for a maximum of eight CTI Managers in a cluster. Cisco recommends that you load-balance CTI applications across the various CTI Managers in the cluster to provide maximum resilience, performance, and redundancy.

Cisco TelePresence T Series The Cisco TelePresence T Series high-definition presentation capabilities and simple controls on a touch display help make your meeting as immersive and natural as possible. See Immersive Telepresence Endpoints.

Cisco TelePresence Touch 12 A touch-panel LCD device that enables you to conduct telepresence meetings without the Cisco Unified IP phone.

See *Installing and Configuring the Cisco TelePresence Touch 12* and the *Cisco TelePresence Touch 12 User Guide* for more information.

Cisco Unified Communications Manager Unified CM. Application that extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones and multimedia applications. Open telephony application interfaces make possible services such as multimedia conferencing and interactive multimedia response systems. See also CUCM.

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

codec The “brain” of the CTS. The primary codec connects with the network and Cisco Unified Communications Manager (Unified CM) to perform call management functions for the system. The secondary codec performs processing for the system elements that are attached to them. The optional presentation codec supports the document camera (if present), auxiliary displays, and works with an auxiliary control unit and audio extension unit for additional audio/video applications. The number and type of codecs your system uses depends on which CTS device you are using.

CTRS Cisco TelePresence Recording Server. Providing HD studio recording capabilities in existing Cisco TelePresence rooms. Recordings can be archived automatically on a schedule or transferred to a digital content management system. The CTRS can deliver Cisco TelePresence recordings to any video-enabled device including PCs, smartphones, and digital signs. CTRS runs on the same reliable Media Convergence Server platform as Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager.

CTS device Cisco TelePresence System (CTS) device: CTS 500, CTS 1000, CTS 1100, CTS 1300, CTS 3000, CTS 3200, CTS 3010, and CTS 3210.

CTS-Manager Cisco TelePresence Manager. Software application that schedules and manages Cisco TelePresence calls using common enterprise groupware such as Microsoft Exchange and Lotus Notes.

CTS Manager PreQualification Assistant The CTS-Man PreQualification Assistant ensures that your pre-configuration set-up is performed correctly. The data that is entered into the Tool Test Configuration forms that are used to verify connections to the servers and to get data from them to be used to configure CTS-Man.

CUCM Cisco Unified Communications Manager. (Unified CM) The phone that controls the CTS is configured and maintained through the Cisco Unified CM Administration interface.

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

D

default gateway A router on a computer network that serves as an access point to another network.

DHCP Dynamic Host Configuration Protocol is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual intervention.

display screen animation System information icons that may be displayed on the Cisco TelePresence System (CTS) main display screen. System information includes call connection status alerts, meeting alerts, and maintenance alerts. These alerts fade from one state to another to show the status of the system.

display screen icon System information icons that may be displayed on the Cisco TelePresence System (CTS) display screen. System information includes call connection status alerts, meeting alerts, and maintenance alerts.

DMP Digital Media Player. Cisco Digital Media Players are highly-reliable, IP-based endpoints that can play high-definition live and on-demand video, motion graphics, web pages, and dynamic content on digital displays, usually an LCD Professional Series display or any other directly attached television screen, monitor, or projector (analog or digital, standard-definition or high-definition) that shows media to an audience. There is an extra input connector for the Digital Media Player (DMP) on your Cisco TelePresence device. See the Cisco Digital Media Players home page on Cisco.com.

See also LCD.

DN Directory number.

DNS Domain Name System. System used on the Internet for translating names of network nodes into addresses.

DSCP Differentiated Services Code Point. A field in the header of IP packets for packet classification purposes. DSCP for TelePresence Calls field description: This parameter specifies the DSCP value for Cisco TelePresence calls. This parameter is set to the default value unless a Cisco support engineer instructs otherwise. This is a required field, if present on your system. Default: CS4(precedence 4) DSCP (100000) and is selectable per device.

DVI DVI cables are used for direct digital connections between source video (namely, video cards) and LCD monitors.

E

enbloc dialing Allows you to compose and edit the number to dial on your phone's display before it is sent to the phone system to be dialed.

endpoint Cisco TelePresence System (CTS) endpoint. The combination of hardware and software that comprise a Cisco TelePresence System. The hardware for an endpoint includes a Cisco Unified IP 7900 Series telephone, one or more large-screen meeting displays, plus presentation devices, cameras, microphones, speakers, and in some models, lighting systems.

EWS Exchange Web Services. Managed API that provides an intuitive interface for developing client applications that use Exchange Web Services. The EWS Managed API provides unified access to Microsoft Exchange Server resources, while using Microsoft Office Outlook–compatible business logic. The EWS Managed API communicates with the Exchange Client Access server by means of EWS SOAP messages.

extranet An extranet is a private network that uses Internet protocols and network connectivity. An extranet can be viewed as part of a company's intranet that is extended to users outside the company, usually via the Internet. It has also been described as a “state of mind” in which the Internet is perceived as a way to do business with a selected set of other companies (business-to-business, B2B), in isolation from all other Internet users. In contrast, business-to-consumer (B2C) models involve known servers of one or more companies, communicating with previously unknown consumer users.

An extranet can be understood as an intranet mapped onto the public Internet or some other transmission system not accessible to the general public, but managed by more than one company's administrator(s). For example, military networks of different security levels may map onto a common military radio transmission system that never connects to the Internet. Any private network mapped onto a public one is a virtual private network (VPN), often using special security protocols.

F

fluorescent lamp A lamp that uses electricity to excite mercury vapor in a gas that results in an energy that produces short-wave ultraviolet light. This light then causes a phosphor to fluoresce, producing visible light. Sources of light in most rooms are either incandescent light bulbs that use tungsten filaments or fluorescent lights. Each of these light sources, and the amount of light in terms of lumens or watts, produces a different color temperature. This color temperature is sometimes expressed using terms such cool, warm, or daylight, but can be expressed more precisely in kelvins (K) as a numeric value. When adjusting the images on the display screens for the Cisco TelePresence system, you must take the color temperature of the ambient light in the room into consideration.

full duplex mode Transmission of data in two directions simultaneously.

G

guest operating system An operating system that is installed and run in a virtual machine. In the Cisco TelePresence environment, the CTS Manager, CTMS, and CTRS are guest operating systems. Before you can install the guest operating system, you must obtain the installation media for the operating system and configure the virtual machine to use the CD/DVD drive to access the installation media. See VMware.

gzip GNU zip. Software application used for file compression.

H

H.264/MPEG-4 AVC A standard for video compression. See also MPEG-4 AVC and IDR.

half duplex mode Transmission of data in one direction at a time.

HD High definition display.

HDMI Document camera input and cable.

I

IAB Internet Architecture Board. The IAB is chartered both as a committee of the Internet Engineering Task Force (IETF) and as an advisory body of the Internet Society (ISOC). Its responsibilities include architectural oversight of IETF activities, Internet Standards Process oversight and appeal, and the appointment of the RFC Editor. The IAB is also responsible for the management of the IETF protocol parameter registries.

IDR An IDR frame is a special kind of I frame used in MPEG-4 AVC encoding. IDR frames can be used to create Advanced Video Coding (AVC) streams, which can be easily edited.

Immersive Telepresence Endpoints CTS 3210, CTS 1300, Cisco TelePresence T3. Provides an immersive, interactive in-person experience. See also personal system.

incandescent lamp A lamp that allows an electric current to pass through a thin filament, heating it and causing it to emit light. Sources of light in most rooms are either incandescent light bulbs that use tungsten filaments or fluorescent lights. Each of these light sources, and the amount of light in terms of lumens or watts, produces a different color temperature. This color temperature is sometimes expressed using terms such cool, warm, or daylight, but can be expressed more precisely in kelvins (K) as a numeric value. When adjusting the images on the display screens for the Cisco TelePresence system, you must take the color temperature of the ambient light in the room into consideration.

Internet model (free path) The Internet model is an unsecured "free path" model of packet delivery: Packets are delivered in any way possible and each uncontrolled router on the way to the destination handles how to deliver the packet to the next stop. See VPN model (fixed path).

IP address A device identifier on a TCP/IP network.

J

jitter

jitter call

jitter period

Variation in packet transit delay caused by queuing, contention, and serialization effects on the path through the network. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

Jitter call is the average jitter measurement per call. Shown in the Jitter/Call output field as part of Per Call Jitter and Packet Loss Reporting.

Jitter period is the interval between two times of maximum effect (or minimum effect) of a signal characteristic that varies regularly with time. Jitter frequency, the more commonly quoted figure, is its inverse.

The CTS measures jitter every 10 seconds. The Jitter/Period field reports the jitter measurement for the last 10-second period.

The CTS calculates jitter as the sum of the maximum deviation (both late and early) from the expected arrival time as given by the frame period. CMA computes frame jitter based on the arrival time of the last packet of a frame.

L

LCD Liquid crystal display. The LCD display is an accessory for the Cisco Digital Media Player (DMP) for use in your digital signage network or your enterprise TV network. It is used for displaying video, images, or computer data during a Cisco TelePresence meeting. See the Cisco LCD Professional Series Displays home page on Cisco.com for more information.

See also DMP.

LED Light-emitting diode. Indicators on the CTS that determine whether the user is sitting within camera range.

light temperature A theoretical means of describing visible light that is determined by comparing its hue with a heated black-body radiator. The lamp's color temperature is the temperature in kelvins at which the heated black-body radiator matches the hue of the lamp.

Live Desk The Live Desk is a person who has been assigned to a Cisco TelePresence endpoint to assist you with problems that may occur during a meeting. To connect to Live Desk, press the **Live Desk** softkey. If a Live Desk has not been assigned to your Cisco TelePresence endpoint, the following message is displayed on your phone screen: "There is no Live Desk number configured"

Live Desk is configured in the **Configure > Live Desks** Window of the CTS-Manager Administration interface. See the Cisco TelePresence Manager Installation and Configuration Guide on Cisco.com.

LTRP Long Term Reference Picture.

M

MAC address Media Access Control. A hardware address that uniquely identifies each node of a network.

MIDlets Mobile Information Device Profile (MIDP). A Java application designed to run on resource-constrained devices such as phones, PDAs, intelligent appliances, and the like. A MIDlet (in J2ME) is similar to a Java Applet (in J2SE), but more specialized, efficient, and optimized for limited devices. MIDlets supports graphics and animation, multimedia, touchscreen, networking, persistent data storage, and provides excellent Look And Feel (LAF) integration with the host platform.

The Cisco Unified IP Phone uses MIDlets as part of the Cisco TelePresence System Enhanced Phone User Interface: MIDlets support CTS Cisco Unified IP phone features. Configure MIDlets in the Cisco Unified CM Administration interface for Cisco TelePresence.

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

MPEG-4 AVC A patented collection of methods defining compression of audio and visual (AV) digital data. See also H.264/MPEG-4 AVC and IDR.

multipoint meeting Multipoint is where you are able to connect more than two sites in one video conference. This normally requires a bridge, although some video conference units are also able to connect multiple sites.

MXE Media eXperience Engine. The Cisco Media Experience Engine is a modular media processing system that provides interoperability between Cisco TelePresence and video conferencing devices, extending the reach of collaboration and communication within organizations. MXE provides 720p interoperability with video conferencing.

Configure MXE in CTS-Manager. See also Cisco TelePresence Firewall and Access List Considerations for support information for Cisco TelePresence.

N

nonce A nonce value (a random number that supports digest authentication) is used to calculate the MD5 hash of the digest authentication password.

Non-permitted User Cisco WebEx user role configured in the CTS Manager Administration interface. These users are not permitted to request Cisco WebEx; no Cisco WebEx meeting options are available to these users. See Permitted User.

O

One-Button-to-Push Allows you to press the meeting that is listed on the in-room CTS Cisco Unified IP phone to start a Cisco TelePresence meeting.

Option 150 Recommended during Dynamic Host Configuration Protocol (DHCP) Server configuration so that Windows 2000 can work with the Cisco IP Telephony solution. Unified CM devices boot up and request an IP address. When you create a new scope in the DHCP server and add a TFTP option to the scope, you are prompted to add the default gateway and the TFTP Server IP Address (Option 150). Option 150 can contain more than one IP address, which can be used for TFTP redundancy.

P

PoE Power over Ethernet.

P-frame An easily compressible video frame type. A video frame is compressed using different algorithms that allow varied amounts of data compression. These different algorithms for video frames are called picture types or frame types. The three major picture types used in the different video algorithms are I, P, and B.

Permitted User Cisco WebEx user role configured in the CTS Manager Administration interface. These users are permitted to request Cisco WebEx for specific meetings using CTS Manager. See Non-permitted User.

personal system Personal Cisco TelePresence System. The virtual, in-person experience of Cisco TelePresence directly into the private office. The CTS 500 and CTS 1000 are considered to be personal systems. See also Immersive Telepresence Endpoints.

PiP Presentation-in-Picture. Data or graphics content are shared through the same display in which conference participants are displayed.

PoE Power over Ethernet.

point-to-point meeting The direct connection of two sites in a video conference. This only works if both sites use the same type of connection (either IP or ISDN).

Premium User Cisco WebEx user role configured in the CTS Manager Administration interface: Cisco WebEx is always on. Controlled on the CTS Manager LDAP configuration page.

presentation codec The presentation codec provides 30 frames per second to support full-motion video presentations between Cisco TelePresence endpoints.

Presenter Cisco WebEx user role configured in the CTS Manager Administration interface: A Presenter shares presentations, specific applications, or the entire desktop. The Presenter controls the annotation tools and can grant and revoke remote control over the shared applications and desktop to individual Attendees.

primary codec The primary codec is the primary unit; it communicates with secondary units, sends and receives packets on the uplink network. It contains an onboard Gigabit Ethernet switch. For example, in a CTS 3000 or CTS 3200 system, the primary codec controls two secondary codecs as well as many system components and the graphical user interfaces. In a Cisco TelePresence 1000, it controls all system functions.

PCB Printed circuit board.

R

RFC Request for Comments. Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards.

S

scheduled meeting Multipoint TelePresence meetings are scheduled by end users using Microsoft Exchange or IBM Domino clients in the same manner that a point-to-point meeting is scheduled. Scheduled meetings require no CTMS administrator interaction. CTS Manager is a required component for scheduled meetings. It provides the interface between Microsoft Exchange or Lotus Domino and the CTMS, allowing the appropriate resources on the CTMS to be reserved for the multipoint meeting.

screen resolution The fineness of detail that can be presented in the image on the CTS main display screen. Recommended screen resolution for Cisco TelePresence is 1024 x 768.

SD Standard definition display.

secondary codec Codecs that assist the primary codec in the large Cisco TelePresence 3000/3200 systems. Secondary codecs process audio and video signals and send them to the primary codec, which multiplexes the signals into separate, single RTP streams.

Self View Enables you to see yourself on the main display before your meeting starts.

single system A Cisco TelePresence System featuring a single display screen.

SHA Secure Hash Algorithm. A set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2.

SIP Session Initiation Protocol. Protocol designed to signal the setup of voice and multimedia calls over IP networks.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks as a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. See the Cisco TelePresence System Message Guide.

SOAP Simple Object Access Protocol. XML-based protocol to let applications exchange information over HTTP.

spirit level Spirit level or bubble level is an instrument designed to indicate whether a surface is level or plumb. A spirit level is included with the CTS 1300 camera kit.

SSCD System Status Collection Daemon. The daemon gathers statistics about the system it is running on and stores this information. Those statistics can then be used to find current performance bottlenecks (performance analysis, for example) and predict future system load (capacity planning, for example).

static meeting Non-scheduled meetings configured on the Cisco TelePresence Multipoint Switch (CTMS) through the administration interface. A meeting scheduler or administrator, who sets up the static meeting, manually assigns a meeting access number that is used to access the meeting. See ad hoc meeting.

supported Internet browser Cisco administration interfaces support Internet Explorer version 6. You can use Internet Explorer versions 6, 7, or 8, or Firefox version 3.x with the CTS 500 32".

switching mode CTS Manager configuration. CTS 3000 and CTS 3200 endpoints only.

Auto-Assign—Switching mode is determined by the default CTMS policy, which is configured in System **Configuration > Policy Management** page of your CTMS setup.

Room—All the participant displays of the endpoint are switched each time the meeting participant who is speaking changes to a meeting participant at a different endpoint.

Speaker—Only the corresponding participant display (left, center, or right) is switched; the remaining participant displays are not switched. Using the speaker switching mode provides the ability to view up to three different remote endpoints at the same time.

Sysop System Operation (sysop) Logs. Sysop messages describe system activity. Some messages can help you identify and resolve system operation problems. These messages are available to the user from the CTS Administration interface. See the "Managing Log Files" section of the troubleshooting chapter for your CTS device.

Syslog System Logs (syslog). Debugging logs that are collected from your system and used by Cisco technical response to diagnose and resolve issues. These messages are not ordinarily seen by the user.

T

TFTP Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

TIP Telepresence Interoperability Protocol. The TIP Specification provides a protocol for interoperability between videoconferencing products, including streaming of audio, video, and data to and from videoconferencing products.

This feature adds TIP 7 support to the CTS and CTMS 1.7 release. The main purpose of the feature is for CTS and CTMS to operate in a strict TIP V7 mode when communicating with devices advertising TIP V7 support. This feature adds the ability to differentiate between MUX and TIP modes of operation to help with the strict adherence to the TIP V7 specifications as well as improving debugging and other operational processes. This feature adds the ability for the CTS to be configured for operation in a TIP-only mode and configured with a set of media features typically not used in Cisco-only deployments. This helps the CTS and CTMS inter-operate with third-party TIP devices.

TIP allows only endpoints with Restricted media settings to join Cisco TelePresence meetings. TIP endpoints are expected to be able to send restricted media and to drop endpoints that can only transmit un-restricted media. See the Telepresence Interoperability Protocol for Developers home page on Cisco.com.

trap A Simple Network Management Protocol (SNMP) trap is a message which is initiated by a network element and sent to the network management system. See the Cisco TelePresence System Message Guide.

triple system A Cisco TelePresence System featuring three display screens.

U

UDI Unique device identification.

V

VGA Video Graphics Array port and cable for Cisco TelePresence. A CTS endpoint initiates a presentation at any point by plugging the VGA Auxiliary cable into the CTS endpoint presenter's laptop, which automatically shares from the presenter’s laptop. The last participant in the meeting to plug in their laptop with the VGA cable shares their presentation using PiP. See the Cisco TelePresence System User Guide for more information about sharing presentations.

virtual machine A virtual machine (VM) is a software implementation of a machine (a computer, for example) that executes programs like a physical machine does. A system virtual machine provides a complete system platform which supports the execution of a complete operating system (OS). See the Cisco TelePresence System Commercial Express Installation Guide on Cisco.com for more information.

VLAN ID The identification of the virtual LAN, which is used by the standard IEEE 802.1Q. Being on 12 bits, it allows the identification of 4096 VLANs.

VMware

VMware software provides a completely virtualized set of hardware to the guest operating system. VMware software virtualizes the hardware for a video adapter, a network adapter, and hard disk adapters. The host provides pass-through drivers for guest USB, serial, and parallel devices. In this way, VMware virtual machines become highly portable between computers, because every host looks nearly identical to the guest. In practice, a system administrator can pause operations on a virtual machine guest, move or copy that guest to another physical computer, and there resume execution exactly at the point of suspension. Alternately, for enterprise servers, a feature called VMotion allows the migration of operational guest virtual machines between similar but separate hardware hosts sharing the same storage. Each of these transitions is completely transparent to any users on the virtual machine at the time it is being migrated.

See the Cisco TelePresence System Commercial Express Installation Guide on Cisco.com for more information.

VPN model (fixed path)

The VPN model uses a fixed, more secure path for packet delivery. VPNs only allow authorized personnel to gain access to their network. See also Internet model (free path).

W

WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) is a set of methods based on the Hypertext Transfer Protocol (HTTP) that facilitates collaboration between users in editing and managing documents and files stored on World Wide Web servers. WebDAV was defined in RFC 4918 by a working group of the Internet Engineering Task Force (IETF).

WebEx

Cisco WebEx collaboration tools combine real-time desktop sharing with phone conferencing. See the Cisco TelePresence WebEx OneTouch Configuration Guide for the Cisco TelePresence System for first-time setup information.

A

B

C

D

F

H

I

L

M

N

P

R

S

T

U

V